Universidad Zaragoza
1542

Trabajo Fin de Grado

Bitcoin: las claves de la moneda virtual

Autor

Álvaro Seguí Iglesia

Directora

Begoña Gutiérrez Nieto

Facultad de Economía y Empresa

2013

ÍNDICE:

Índice de gráficos

1. INTRODUCCIÓN

El objetivo del trabajo es analizar la moneda electrónica de reciente creación, el Bitcoin (BTC), que últimamente está haciéndose más popular y parece que se afianza como una moneda fiable a la hora de realizar transacciones. Asimismo su cotización oscila, desde la subida de abril, alrededor de los 100€, fluctuando entre los 60 y los 130€.

Al tratarse de un nuevo sistema de pago se analizará la evolución de la moneda desde su creación en 2009 hasta la actualidad. Se estudiará su funcionamiento (a través de transacciones, bloques, minería, etc.), así como las fluctuaciones del Bitcoin, la configuración y propiedades de las operaciones, sus aplicaciones y las oportunidades de futuro existentes entre otros puntos. También veremos las oportunidades y riesgos que entraña el uso del Bitcoin, así como los efectos positivos y negativos que puede tener en la economía global.

En concreto trataremos los siguientes aspectos. Primero, se hará una visión histórica del origen y evolución de la moneda. A continuación se estudiarán algunos aspectos técnicos del Bitcoin, en concreto su naturaleza P2P y las técnicas de encriptación que conlleva. En el apartado 5 se analizará el funcionamiento de las transacciones con Bitcoins (bloques, cadena de bloques) así como la creación de la misma (minería). Posteriormente analizaremos más profundamente las operaciones que se llevan a cabo, determinando su configuración así como las propiedades inherentes a las mismas, estudiaremos los riesgos y ventajas que presentan (anonimato, transparencia, volatilidad, etc.). En el siguiente apartado se describirá la cotización y fluctuación del Bitcoin desde su creación y el impacto económico que ha supuesto. En el apartado 9 se estudiarán las aplicaciones del Bitcoin a nivel personal y empresarial para continuar analizando las oportunidades de futuro que se presentan en el apartado 10. A continuación se relacionará esta moneda con las autoridades monetarias y bancos para analizar su desregularización y posibles consecuencias. En el último apartado se abordan aspectos particulares de esta nueva moneda que a día de hoy se desconocen sus efectos, como por ejemplo si se puede tratar de una burbuja económica, si se trata de un sustituto del dinero físico, si se evitará la inflación, etc. Terminaremos el trabajo adjuntando unos anexos, las conclusiones y las referencias utilizadas a lo largo del mismo.

2. MOTIVACIÓN

Los motivos para elegir este tema surgieron cuando me informaron sobre este nuevo método de compra-venta en internet. Mi interés me llevo a estudiar en qué consistía y a partir de ahí empecé a informarme en internet y a leer artículos ya que es un tema de actualidad y que cada día aparecen nuevas noticias. Me puse en contacto con el BIFI (Instituto Universitario de Investigación Biocomputación y Física de Sistemas Complejos), en particular con Yamir Moreno, Alejandro Rivero y Francisco Sanz. Junto a ellos he aprendido el funcionamiento del Bitcoin y se han puesto a mi disposición para ayudarme y explicarme cualquier punto de este complejo mundo. Hemos compartido tardes de discusión e investigación donde he podido aprender mucho acerca del tema, lo cual me ha motivado a, en un futuro no muy lejano, seguir investigando y profundizando en el Bitcoin con perspectivas de alcanzar un nivel superior de conocimiento, ya que para este trabajo he tenido que sintetizar las ideas más importantes y no he podido profundizar lo suficiente debido a la amplitud de posibilidades y las limitaciones asociadas al Trabajo de Fin de Grado.

3. ORIGEN

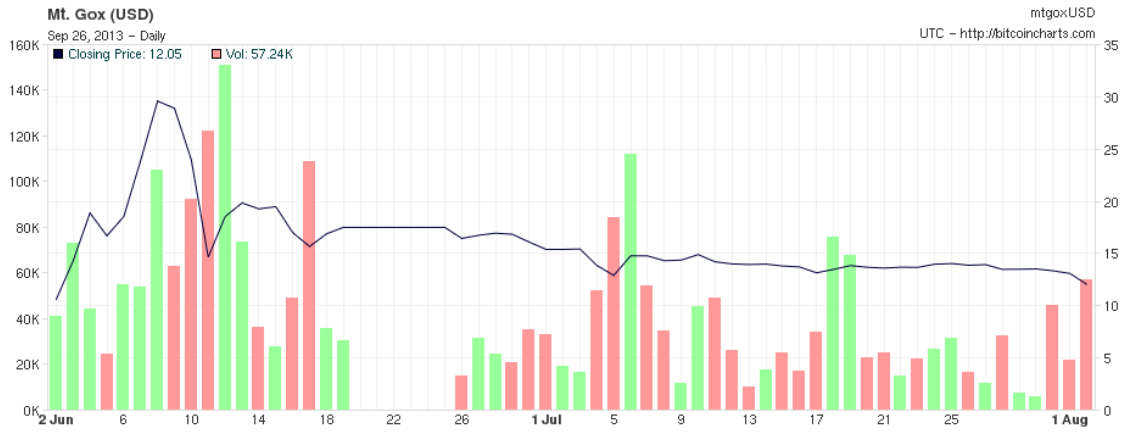
La primera mención del concepto de criptomoneda aparece en 1998 por Dai Wei en el texto *Bmoney* sobre el anonimato (1). En este texto se sentaron las bases y el concepto de moneda electrónica y como resultado surge el Bitcoin que será una de las primeras implantaciones.

Diez años después se registró el proyecto Bitcoin, el 9 de noviembre de 2008, y se publica el artículo *Bitcoin: un sistema electrónico de efectivo Peer-to-Peer* (2) donde se describen los primeros conceptos detrás de Bitcoin y constituye a la primera versión de software Bitcoin. Se trata de la primera especificación del protocolo y prueba de concepto de Bitcoin que fue publicada bajo el pseudónimo de Satoshi Nakamoto (no se sabe si se trata de una persona o grupo de personas, véase por ejemplo (3)). Pero no se puso en marcha hasta dos meses después, el 3 de enero de 2009, cuando se genera la red P2P de Bitcoin y se crea el bloque Génesis (4) (se denomina bloque al conjunto de transacciones registradas cada 10 minutos). Se publica el primer cliente y se crean los primeros Bitcoins dando lugar a la primera transacción de comercio electrónico descentralizado donde las operaciones no se canalizan a través de entidades bancarias u otras empresas financieras que gestionen el seguimiento de las transacciones.

Hacia finales del año 2010 Satoshi Nakamoto deja el proyecto anunciando que se había pasado a trabajar en otras cosas. El creador de Bitcoin nunca reveló su identidad y simplemente dejó su invento al mundo. El origen y la motivación detrás de Bitcoin sigue siendo, hasta hoy, un gran misterio.

Desde 2010, la comunidad Bitcoin ha crecido con muchos programadores trabajando en el proyecto y ha ganado muchos adeptos. Durante junio y julio del 2011 Bitcoin ganó repentinamente la atención de los medios de comunicación dando lugar a compras masivas. De este modo alcanzó los 32$ para caer hasta los 10$ en tan solo 4 días como podemos observar en el gráfico 3.1. El resultado de esta "burbuja" se desinfló lentamente en la última parte del 2011, pero el valor de Bitcoin se recuperó nuevamente hasta superar el pico del 2011.

Gráfico 3.1: "Burbuja" en el mercado de Bitcoin 2011



Fuente: http://bitcoincharts.com/

El 27 de septiembre de 2012, la Bitcoin Foundation (grupo defensivo del Bitcoin vinculado con el negocio de la moneda) fue creada en un esfuerzo por estandarizar, proteger y promover el Bitcoin.

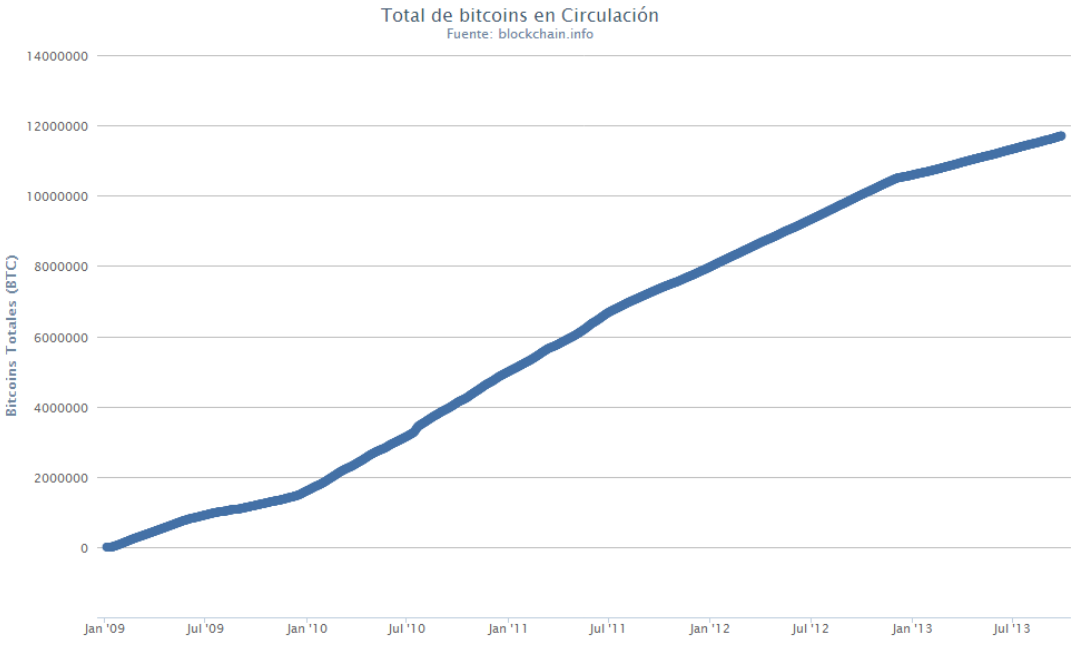
En 2013 se produjo la otra gran burbuja, como podemos observar en el gráfico 3.2, donde alcanzó valores de hasta 180$ para desplomarse después hasta los 60$ que coincidió con el rescate chipriota y del euro y los inversores empezaron a ver esta moneda virtual como una moneda refugio.

Gráfico 3.2: “Burbuja” en el mercado Bitcoin 2013

Fuente: http://bitcoincharts.com/

Actualmente, se calcula que existen 11,7 millones de Bitcoins en circulación en todo el mundo, como refleja el gráfico 3.3, que se estima alcanzan un valor de 1220 millones de euros con una media de 50.000 transacciones diarias. Son ya miles las empresas que aceptan esta divisa virtual como medio de pago. Hoy en día, la economía Bitcoin se está desarrollando rápidamente con nuevos usuarios que se unen a diario.

Gráfico 3.3: Total de Bitcoins en Circulación



Fuente: http://blockchain.info/es/charts

Basándose en la idea de que el dinero es como un medio de intercambio, por lo general en forma de billetes y monedas, que es aceptado por una sociedad para el pago de bienes, servicios y todo tipo de obligaciones, Bitcoin se ha diseñado en torno a la idea de una nueva forma de dinero que usa criptografía para controlar su creación y transacciones, en lugar de depender de autoridades centrales.

4. CARACTERÍSTICAS Y PROPIEDADES

A grandes rasgos, esta nueva moneda se caracteriza por lo siguiente (5).

4.1 CARACTERÍSTICAS ECONÓMICAS

- ✓ Las transacciones son irreversibles.
- ✓ Las transacciones se transmiten en cuestión de segundos y son verificadas en un plazo de 10 a 60 minutos.
- ✓ Se puede cambiar a otras monedas: euros u otras divisas y viceversa, como cualquier moneda.
- ✓ Límite de emisión fijo cercano a los 21 millones de Bitcoins.
- ✓ Desde mayo de 2013 la principal casa de cambio de la red MTGOX requiere verificar las cuentas Bitcoin para evitar problemas de lavado de dinero y otras actividades delictivas.

4.2 CARACTERÍSTICAS TÉCNICAS

- ✓ Los Bitcoins se pueden transferir entre nodos (cada servidor de la red Bitcoin) arbitrarios en la red.
- ✓ El doble gasto (uso simultáneo de Bitcoins en dos operaciones diferentes) se evita mediante el uso de una cadena de bloques.
- ✓ Las transacciones se pueden recibir en cualquier momento, independientemente de si el ordenador de alguno de los agentes está encendido o apagado.
- ✓ Los Bitcoins son divisibles hasta 8 posiciones decimales dando un total de aprox. 21×1014 unidades monetarias.
- ✓ Las transacciones son baratas, y generalmente gratuitas.
- ✓ El procesamiento de transacciones y la emisión del dinero se realizan colectivamente a través de la minería (entendido como el proceso de creación de bloques de Bitcoin).

4.3 CARACTERÍSTICAS COMERCIALES

- ✓ Está descentralizada: no es controlada por ningún Estado, banco, institución financiera o empresa.
- ✓ Es imposible su falsificación o duplicado gracias a un sofisticado sistema criptográfico.
- ✓ No hay intermediarios: las transacciones se hacen directamente de persona a persona.
- ✓ No es necesario revelar la identidad del usuario al hacer negocios y de este modo se preserva la privacidad del mismo.
- ✓ El dinero le pertenece al 100%; no puede ser intervenido ni las cuentas pueden ser congeladas.

4.4 PROPIEDADES

Al estar limitada la producción de Bitcoins se evita la depreciación del mismo y al contar con la subdivisión hasta en microbitcoins mantendrá su poder económico al contrario de lo ocurrido con el dólar por ejemplo.

Las unidades van desde el Bitcoin hasta:

mBTC= milibitcoin= 0.001 Bitcoin

µBTC=microbitcoin=0.000001 Bitcoin

Sathosi= 0.00000001 Bitcoin (es la subdivisión más pequeña)

La creación de la moneda va asociada a la creación de cada bloque. Se comenzó por 50 Bitcoin por bloque generado, cuando se alcanzaron los 210000 bloques se pasó a la mitad, 25 Bitcoin, cuando se alcancen 420000 bloques de Bitcoins se pasará a la mitad y así sucesivamente hasta llegar al límite fijado de 21 millones de Bitcoins.

Una vez se alcance la cifra de los 21 millones de Bitcoins para poder asegurarnos que la transacción esté en el próximo bloque se pagará una mínima comisión mientras que actualmente como hemos comentado anteriormente son gratuitas, aunque existe la posibilidad de pagar una comisión.

Además se caracteriza por que la moneda no ha sido falsificada y en cuanto a prácticas fraudulentas sólo se han detectado ataques a monederos o se han infectado ordenadores ajenos para ponerlos a fabricar monedas, los cuales fueron solucionados.

4.5 ESTADÍSTICAS

La red ha estado en funcionamiento durante más de 55 meses sin problemas, ofreciendo un nivel de seguridad impresionante. Matemáticamente es infranqueable, de lo contrario las personas de todo el mundo no depositarían su confianza en la moneda. Además, si en un futuro llegaran a existir algoritmos de cifrado (hash) más viables y seguros, el sistema Bitcoins podría ser actualizado y hacer uso de la tecnología más novedosa del momento, garantizando siempre una seguridad óptima. Ha habido un crecimiento comercial y de uso especialmente significativo en el último año. Hasta septiembre del 2013, estas son algunas estadísticas:

- ✓ Larga cadena de bloques creados (más de 250.000 bloques).
- ✓ Una gran cantidad de potencia de procesamiento para asegurar las transacciones - estimado en más de 25 terahashes/s.
- ✓ Más de un millón de euros de volumen de comercio diario distribuidos en 50.000 transacciones.
- ✓ El valor total de todos los Bitcoins en circulación es de más de 1220 millones de euros.
- ✓ Sólo se han registrado dos incidentes, uno de seguridad importante en el protocolo (solucionado en Agosto del 2010) y el otro debido a la aplicación android (6), también solucionado.

4.6 VENTAJAS Y DESVENTAJAS

Partiendo de los puntos que acabamos de analizar podemos concluir las ventajas y desventajas de este sistema de pagos.

Ventajas:

- ✓ Tiene un límite de emisión que llegará a 21 millones lo que la convierte en una moneda que tiende a apreciarse frente a otras. El dólar perdió el 90% de su valor en 50 años, como consecuencia de la creciente emisión, sin embargo el Bitcoin garantiza que la emisión tendrá tope.

- ✓ Una moneda con restricción de emisión se traduce en deflación de precios, es decir, un bien comprado hoy con Bitcoin sería más caro que si se compra más adelante, porque el valor de la moneda va hacia la apreciación.
- ✓ Al estar controlado de forma automática el sistema de creación de Bitcoins, hace que la oferta de dinero sea limitada, lo que controla la inflación de un modo similar al patrón oro.
- ✓ Es una moneda "anónima", no la puede controlar un gobierno, ni una entidad. En un punto se parece al sistema previo a la aparición de los Bancos Centrales, donde cada entidad respaldaba sus emisiones con sus propias reservas. Al no estar regulada por un organismo es menos manipulable, porque intervienen tantos actores que resulta imposible lograr que todos acuerden una acción común.
- ✓ No es necesario pasar por un banco o intermediario para formalizar una transacción. Esto significa que las comisiones por transacción son mucho más bajas.
- ✓ No son necesarios pre-requisitos para poder obtener una cuenta en Bitcoin.
- ✓ El control de las transacciones es realizado por todos los participantes del ecosistema Bitcoin, cada operación queda completamente registrada, de tal manera que cualquiera puede ver movimientos, aunque sin poder detectar quién los hace.
- ✓ Las transacciones se hacen en tiempo real. Cualquier transferencia convencional de dinero de un país a otro suele demandar entre 24 y 72 horas (además de las comisiones cobradas). Esta moneda se transfiere en tiempo real de una cuenta a otra y sin comisiones. Los Bitcoins son transferidos directamente de persona a persona a través de la red.
- ✓ Valor no manipulable: al ser una moneda descentralizada por todos sus usuarios, el valor del Bitcoin no puede ser manipulado. Por lo tanto no hay riesgos de inflación de esta moneda.
- ✓ Difícil falsificación: se debe a la base de datos distribuida entre todos los usuarios de Bitcoin. En el caso de que se falsificara, algo extremadamente difícil, sólo se podría falsificar una vez por una transacción.

Desventajas:

- ✓ Enorme fluctuación en su valor contra otras monedas.
- ✓ No hay garantías de que se convierta en una moneda aceptada por todos. Si la tendencia actual cambiara y los usuarios dejaran de usarla, el valor del Bitcoin se acercaría a cero.
- ✓ La falta de un regulador del ecosistema (entendiéndolo como el conjunto de operaciones, agentes, volumen de Bitcoins, etc.) explica en gran medida la volatilidad. Como depende exclusivamente de la oferta y la demanda, se corre el riesgo de que sus variaciones desalienten el uso.
- ✓ El anonimato que garantiza el sistema no permite saber quiénes están detrás de las operaciones. De esta manera, un gobierno no podría detectar a un profesional independiente que cobrara sus servicios en Bitcoin para cobrarle impuestos, pero tampoco detectaría a un narcotraficante.

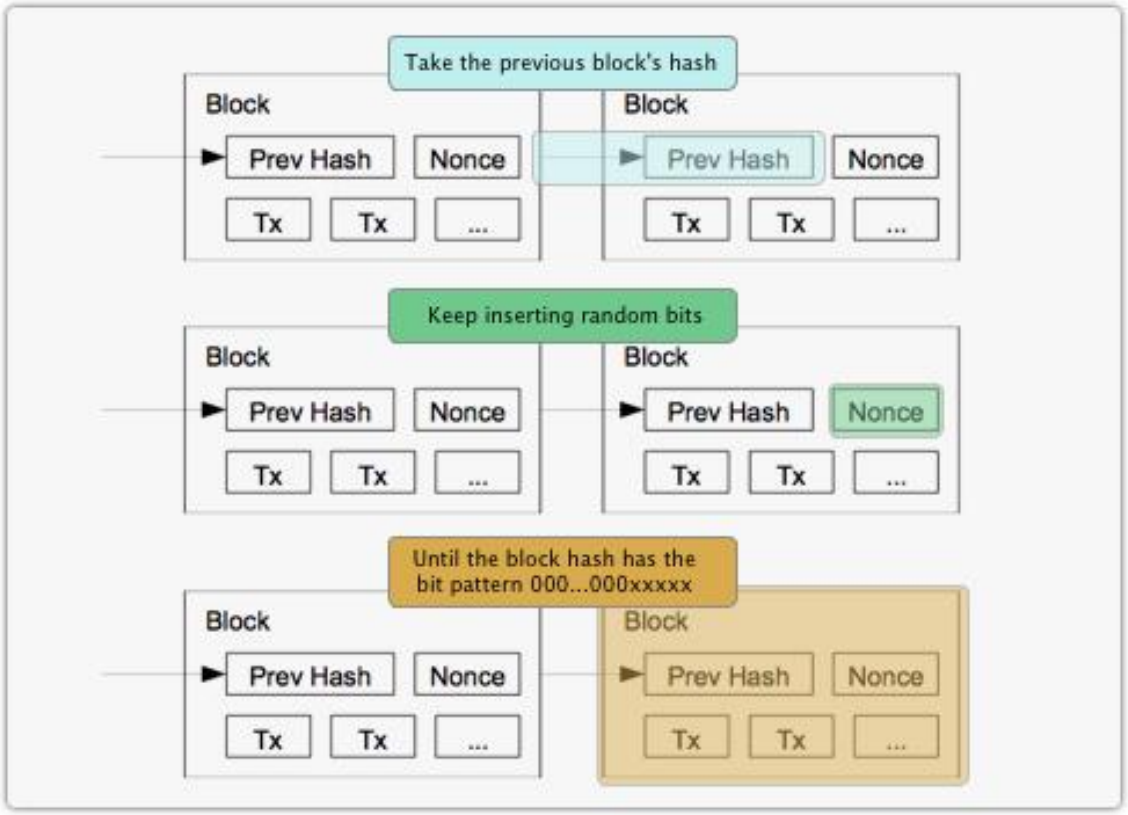
5. FUNCIONAMIENTO (7)

5.1 BLOQUES Y ENCRIPTACIÓN (9)

Los Bitcoin se encuentran en lo que se llaman bloques, que se generan entre todos los nodos de la red. Cuando un nodo de la red genera un bloque, automáticamente gana 25 Bitcoin como veremos en el apartado 5.3 Minería.

Todos los datos son grabados permanentemente en la red Bitcoin a través de bloques. En el gráfico 5.1 podemos observar que estos bloques contienen las últimas transacciones (Tx), un nonce (número aleatorio) y el hash de la secuencia anterior (8). Aproximadamente se genera un bloque cada 10 minutos y se unen a la cadena de bloques a través de la minería.

Gráfico 5.1: Elementos de un bloque



Fuente: http://goo.gl/nU22bu

Para la generación de un bloque lo que se pide es generar un SHA-256 (Secure Hash Algorithm) que está formado por 256bits con 64 caracteres hexadecimales. Se indica la dificultad del bloque a generar que viene determinado por la cantidad de ceros que deben aparecer al inicio del hash. Es decir, un hash de dificultad 7, irá precedido de siete ceros, uno de dificultad 12, de doce ceros, etc.

Ej: 0000000000000016b155434b26c45406284d447d8b51b52142c61aa559242b87

Se trataría de un hash de dificultad 14.

La red trata de crear seis bloques por hora (como hemos comentado cada 10 minutos), y cada 2016 bloques (alrededor de dos semanas) todos los clientes Bitcoin comparan el número real de bloques creados con el objetivo de los que tendrían que haberse creado para así ajustar la dificultad (aumentar o disminuir) de generación de bloques para que el suministro total de Bitcoins no supere la cantidad de 21 millones.

Así pues, una vez definida la dificultad necesaria para la creación del siguiente bloque, los mineros (aquellos que crean los bloques) se ponen a generar hash probando cada vez

un número aleatorio o nonce hasta que uno de ellos consigue la dificultad exigida y se le da la generación del bloque por lo que se crean 25 BTC (originalmente eran 50BTC pero se divide por 2 cada 210.000 bloques generados, cada 4 años más o menos, hasta que se llegue al límite de producción de BTC creados). Además de estos 25BTC suele haber un diferencial positivo de BTC en concepto de comisiones que pueden pagar diferentes firmas de transacciones que quieren asegurarse estar en el siguiente bloque.

Esta es la primera operación del bloque y es especial puesto que se crean BTC para la persona que lo generó. Una vez alcanzado el límite anteriormente comentado las operaciones se basarán en las comisiones para que sean aceptadas las transacciones.

El nonce o número aleatorio se trata de un número utilizado una única vez que firma cada hash generado en el bloque hasta que le da al mismo la cantidad deseada de ceros. Se utiliza uno diferente cada vez porque si no en el siguiente bloque (de la misma dificultad) se generaría el mismo hash.

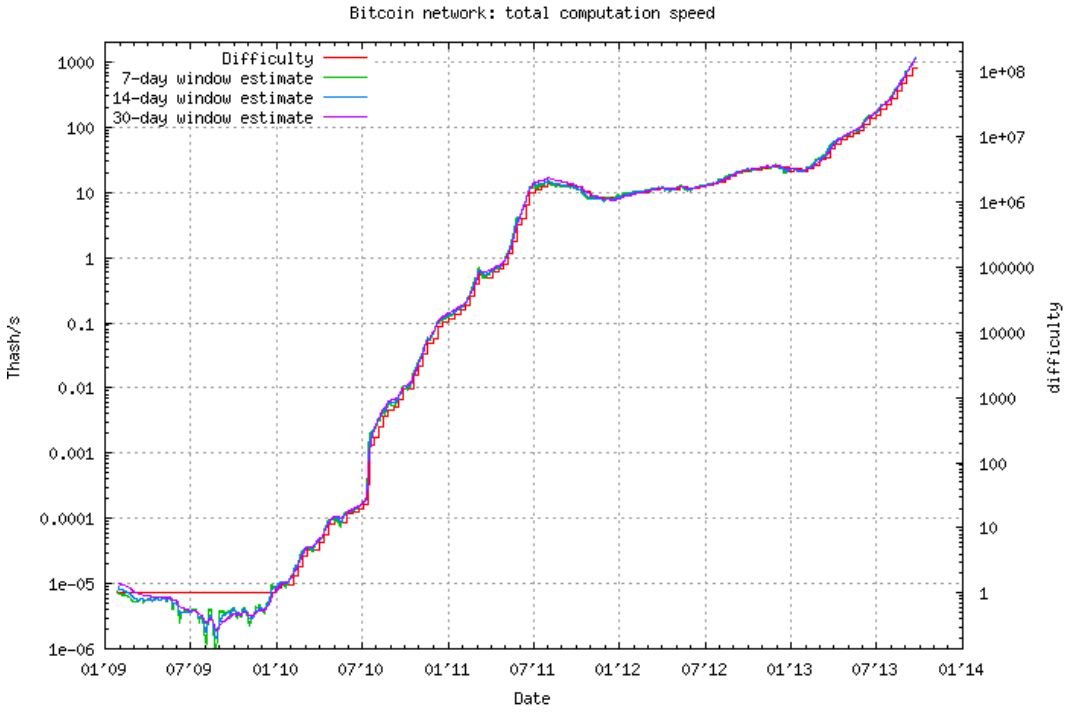
Un bloque se considera resuelto, es decir es publicado y considerado válido por el resto de nodos, cuando se consigue el hash SHA-256 de la dificultad exigida y se han recogido y agregado las transacciones de los últimos diez minutos al bloque en que están trabajando.

A modo de resumen basta con aplicarle una función matemática resumen (hash) al bloque. Se usa para ello la función hash SHA256, que tiene muchas aplicaciones criptográficas. Es decir, si la función es H y el bloque es B, solamente hay que calcular H(B). Pero esa función es fácil de calcular, así que hay que complicar el problema. En este punto, hay dos propiedades de la función hash que nos resultan de interés. Una: si B cambia siquiera en un bit, el resultado H(B)=h es totalmente distinto (al menos la mitad de los bits de h cambian). Dos: conocido h, no podemos extraer información sobre B.

Aprovechando esas propiedades, lo que se hace es añadir al bloque B un paquete de datos aleatorio N, de forma que realmente hay que calcular h=H(B+N). Cada minero probará con valores distintos de N, y el que gana es el que obtenga un valor de h que tenga una cierta forma. Concretamente, el ganador de los bitcoins será el primero que consiga un valor de h que comience con un número determinado de ceros, es decir, H(B+N)=00000000…. El número de ceros determina la dificultad de la tarea, y la idea es ir ajustando la dificultad para que el suministro total de bitcoins no supere la cantidad

de 21.000.000. Cualquier usuario puede crear moneda haciendo uso de la CPU que hay en su ordenador.

Gráfico 5.2: Dificultad para realizar un bloque



Fuente: http://bitcoin.sipa.be/

5.2 CADENA DE BLOQUES

La cadena de bloques engloba todos los bloques generados desde que se creó el bloque génesis hasta el día de hoy (9). Cuando un usuario se introduce en el sistema Bitcoin se descarga en su computadora el historial de bloques desde la creación del sistema.

En Bitcoin Block Explorer (www.blockexplorer.com) o Blockchain Info (www.blockchain.info/es) se muestran los últimos bloques de la cadena de bloques así como todos los anteriores ya que contiene el historial confirmado de todas las transacciones que han tenido lugar en el sistema (4). Se puede comprobar cuántos bloques se han generado en la última hora, el número de transacciones que se han llevado a cabo en cada bloque, la cantidad total transferida en cada bloque e información adicional que permite ver la actividad del sistema.

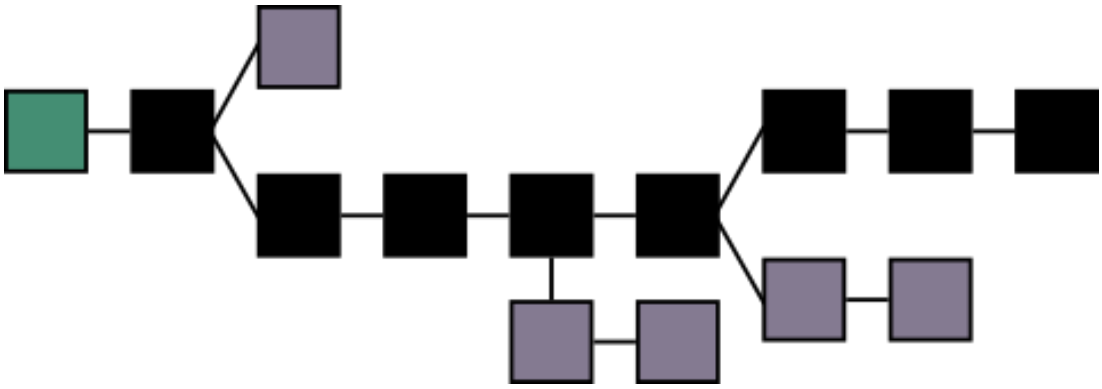
Incluso podemos entrar en cada uno de estos bloques donde aparecerá el hash del bloque que comienza por una determinada cantidad de ceros que es lo que hace que sea tan difícil su elaboración. Para conseguir este bloque el ordenador tuvo que probar muchos valores "nonce" hasta que encontró uno que generó esta cantidad de ceros.

Además cada bloque tiene una línea que pone "Previous block" donde aparece el hash del bloque anterior, el que le precede, y así es como se genera la cadena de bloques.

Al entrar en cado uno de estos bloques podremos ver todas las transacciones contenidas en el mismo y la primera transacción del bloque refleja los ingresos ganados por el ordenador que generó este bloque, es decir, la cantidad generada de la nada por la creación del bloque (ahora mismo 25 Bitcoin) así como las comisiones sobre otras transacciones del mismo bloque que se han querido asegurar su presencia.

Incluso se puede entrar en cualquiera de las transacciones y ver cómo están compuestas, ya que puede haber más de una cantidad que entra y sale.

Gráfico 5.3: Cadena de bloques



5.3 MINERÍA (GENERACIÓN)

Las nuevas monedas son acuñadas mediante la generación de bloques (la generación de un hash) (9). Cuando un bloque es generado se recompensan con una pequeña retribución como hemos explicado en el apartado 4.4 Propiedades.

Se denominda "minería de Bitcoins" al proceso de generación de bloques, los cuales son incorporados en la cadena de bloques y de esta manera se procesan y verifican las transacciones. Pero agregar un bloque a la cadena de bloques es difícil, se requiere tiempo y potencia de procesamiento para conseguirlo como hemos visto anteriormente en el apartado 5.1 Bloques y encriptación donde se explica estos niveles de dificultad y

la complejidad de los SHA-256 y como esta se ajusta para que se produzca un bloque aproximadamente cada 10 minutos.

Así pues, cuantos más mineros haya, mayor será la dificultad para genere un bloque a nivel individual lo que implicará una dificultad total mayor para un atacante, una más difícil sobreescritura del extremo de la cadena de bloques con sus propios bloques (lo que le permitiría el doble gasto de sus monedas).

Para los generadores de los bloques existirá un doble beneficio, por un lado se están beneficiando de los Bitcoins que se les otorga por la creación del bloque así como por las comisiones que pudiesen haber obtenido por parte de algunas transacciones que se quieren asegurar estar en el siguiente bloque.

Cuando se llegue al límite de Bitcoins creados el único beneficio para los creadores de los bloques residirá en las comisiones que cada firma pague para asegurarse estar en el próximo bloque como hemos comentado anteriormente.

Además el trabajo de los mineros permite el mantenimiento de la base de datos de transacciones, lo que es muy importante para mantener toda la información de la cadena de bloques desde que se creó el Bloque Génesis.

Podemos concluir que se premia con Bitcoins a aquellos que contribuyan con la red a la creación de los bloques de la cadena de bloques así como a mantener la base de datos de transacciones.

Existe la posibilidad de "minería en grupo" lo que se conoce como mining pools donde se agrupan muchos mineros para prestar su potencia para la generación de los Bitcoins, así entre muchos usuarios es más fácil generar un bloque que de manera individual. Una vez se genera un bloque el beneficio es repartido entre los participantes de manera proporcional al tiempo y potencia proporcionados. Las *pools* también compiten entre ellos para intenta atraer al mayor número de mineros, hay pools que cobran comisiones cada vez que se genera un bloque y otras que se quedan simplemente con las comisiones procedentes de ese bloque.

Los mineros de Bitcoin son ejecutantes de un programa informático de hardware muy sofisticado, que automatiza el proceso de protección de la red. En resumen, este programa permite:

- ✓ Colectar las transacciones en la red.

- ✓ Validar y no permitir que haya conflicto entre ellas.
- ✓ Agrupar en grandes bloques llamados "cadenas".
- ✓ Calcular una y otra vez "hash criptográficos" hasta que encuentra el adecuado.
- ✓ Envíar el bloque a la red, para añadirlo a la cadena de bloques y ganar una recompensa a cambio.

Las estrategias para la extracción de bitcoins se han ido perfeccionando progresivamente. En los primeros meses de funcionamiento de la red era posible extraer en solitario con una CPU estándar y obtener un bloque y sus 50 BTC asociados con una frecuencia relativamente alta. Posteriormente, la aparición de software de minería adaptado a tarjetas gráficas, mucho más eficiente, desplazó completamente a las CPUs hacia las GPUs. La minería por GPUs se fue profesionalizando, con grandes instalaciones en países con energía barata, configuraciones personalizadas y sistemas especiales de refrigeración. Con el aumento sostenido de la dificultad, los mineros comenzaron a organizarse en grupos independientes para extraer de manera colectiva como hemos comentado anteriormente.

Actualmente, se está comenzando a distribuir FPGAs y ASICs (chips personalizados para realizar un uso en particular, por ejemplo los móviles llevan unos chips ASICsdesarrollado exclusivamente para el uso de los mismo) para extraer bitcoins de manera más eficiente. Si con la minería con CPUs y tarjetas gráficas, el coste de explotación provenía fundamentalmente del gasto energético, la comercialización de equipos especializados de bajo consumo está desplazando las inversiones de los mineros hacia hardware más sofisticado, e indirectamente hacia la investigación necesaria para el desarrollo de estos productos.

5.4 CARTERA

Básicamente la cartera o monedero Bitcoin se refiere al equivalente a un monedero físico pero en la red Bitcoin. Éste puede mostrar el balance total de todas las direcciones Bitcoin que contiene. Además permiten al usuario pagar una cantidad específica a una persona a diferencia de las tarjetas de crédito en las que es el negocio el que cobra.

Estos monederos tienen asociada una clave pública y una privada (ver apartado 6.1 Sistema de claves), la privada sólo es conocida por el dueño y le permite poder usar las monedas que contiene su monedero y la clave pública es usada entre otras cosas para

obtener la dirección de un monedero al cual poderle enviar fondos. Cada monedero lleva asociada una dirección que vendría a ser como el número de cuenta de nuestro banco.

Estas direcciones Bitcoin generadas concretamente proceden de la clave privada (que es la que se utiliza en la firma electrónica) y es la única firma necesaria para poder gastar los fondos asociados a la dirección, pero si se pierde por algún motivo los Bitcoins de esa dirección se pierden para siempre.

El fichero *wallet.dat* representa la cartera electrónica en todas las plataformas. Sin embargo, su seguridad no es total, ya que es posible que keyloggers maliciosos registren las pulsaciones del teclado para capturar la contraseña de cifrado y, en última instancia, tramiten el robo de fondos, por eso es importante tener el ordenador limpio de virus y no hacer uso de la clave privada desde cualquier ordenador.

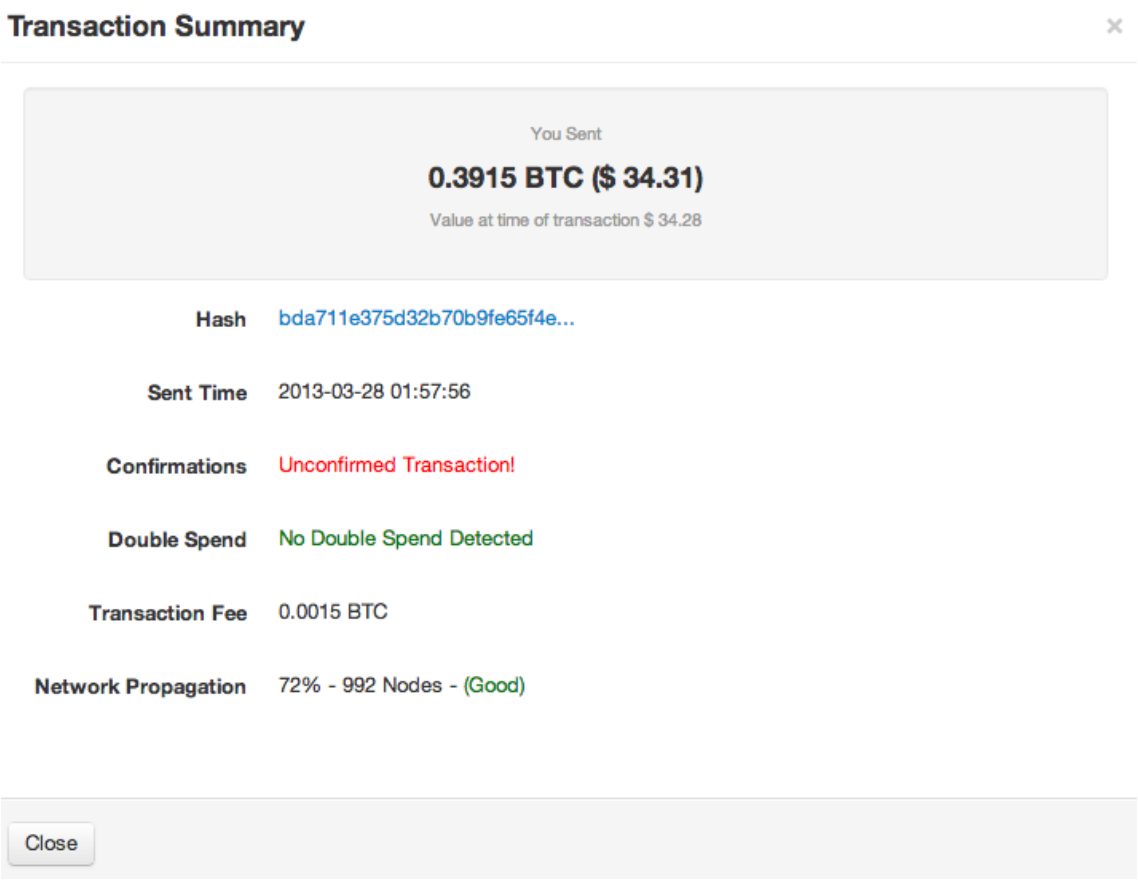
Para poder llevar a cabo transferencias completamente seguras, algunos clientes permiten firmar transacciones en modo desconectado, de forma que las claves privadas nunca estén conectadas a la red, y el riesgo de robo por software malicioso sea nulo.

Por otro lado, el propio protocolo Bitcoin permite el uso de multifirma, que también reduce prácticamente a cero el riesgo de robo de fondos, ya que para poder lanzar una transacción se necesitaría más de una clave privada, que pueden estar guardadas en dispositivos diferentes.

5.5 TRANSACCIONES

Básicamente es como las conocemos, un usuario transfiere algo a otro y para ellos se incluyen Bitcoins en la transacción y son difundidos a los nodos de la red P2P a los que está conectado. Estos nodos validarán las firmas criptográficas y el valor de la transacción antes de aceptarla y retransmitirla.

Gráfico 5.4: Ejemplo de transacción



Fuente: http://bitcoin.stackexchange.com/

6. OPERACIONES

Para entender cómo funcionan las operaciones deberíamos analizar los sistemas de pagos actuales existente y compararlos con los de Bitcoin.

Por un lado tenemos la moneda que no es más que una aleación de cuproníquel, y níquel-latón. O bien, si pagamos con billete, un trozo de papel con un holograma, con una tinta de color y alguna propiedad más que aumenta su seguridad para evitar ser falsificada. Ambos son aceptados a cambio de productos y servicios en el mundo real sin que realmente estén respaldados por un valor como ocurría con el oro.

Por otro lado tenemos a los bancos a los cuales un cliente puede ir con su dinero físico y estos aseguran resguardar el dinero en una "cuenta" de tal forma que puedan disponer de la cantidad que hayan depositado cuando lo deseen. Si lo que se desea es hacer llegar

ese dinero físico que hemos depositado a otra persona el banco se encargará de hacerlo llegar a la entidad receptora por una pequeña comisión, de tal forma que si el receptor consulta el estado de su cuenta aparecerá la transferencia llevada a cabo.

Una vez dicho esto convendría aclarar que hace años el trato con el banco era únicamente personal, pero en los últimos años se ha generalizado el uso de los cajeros automáticos así como las páginas web las cuales registran lo que cada cliente quiere hacer con su dinero (entregar dinero en efectivo, hacer transferencias, consultar fondos, último movimientos, invertir, etc.). La interactuación humana se ha visto muy reducida hasta el punto de fiarnos de los números e información que aparece en los cajeros y ordenadores los cuales aceptamos como papel moneda (algo similar a cuando se comenzó a aceptar papel moneda en lugar de oro o la plata como medio depago).

Independientemente de esta evolución la estructura sigue siendo la misma. Se basa en una autoridad central que mantiene un registro del dinero y a quien pertenece cada cantidad confiando en su honestidad. El cliente podrá disponer del dinero si lo solicita. Además, toda persona debe identificarse ante esta autoridad dando su nombre real con el fin de tener de vuelta su dinero o enviar una cantidad de dinero a otra persona.

Sin embargo el Bitcoin es un sistema de apropiación y de transferencia voluntaria de Bitcoins mediante un proceso similar al de una transferencia bancaria en línea, pero de manera anónima y sin depender de una autoridad central que decida que transferencia realizar y cual no. Estos Bitcoins son valiosos porque generarlos requiere una cantidad de recursos reales (tiempo de CPU y electricidad) y no se pueden arrebatar a una persona sin acceder de manera ilícita a su cartera.

¿Qué seguridad nos da el Bitcoin para llevar a cabo operaciones?

6.1 SISTEMA DE CLAVES:

Para prevenir el robo de los Bitcoins cada firma tiene asociadas dos claves, una pública y otra privada que se almacenan en una cartera, como hemos comentado anteriormente en el apartado 5.4 Cartera.

Clave privada: número secreto que sólo conoce la persona que lo ha generado, puede ser generado aleatoriamente o el usuario puede elegirlo, es decir, puede crearse a través de un texto que podamos recordar.

Clave pública: esta clave como su nombre indica puede ser compartida y está asociada a una clave privada. Puede utilizarse para determinar si una firma es auténtica, es decir, para saber si se ha generado usando la clave privada correcta. Se puede calcular a partir de una clave privada pero no viceversa.

Firma: sirve para demostrar que un usuario concreto ha creado un mensaje, se genera a partir de un hash de algo que debe ser firmado y de la clave privada. A través de un algoritmo usando la clave pública se puede verificar dicha firma.

Así que sólo el usuario con la clave privada puede firmar un documento como una transacción, una compra, etc. para entregarle unos Bitcoins a alguien o para pagar algo en Bitcoins. Por otro lado cualquiera puede validar la firma usando la clave pública del usuario que realiza la transferencia.

Pongamos un ejemplo para entender mejor este proceso:

La Señora Y quiere transferir Bitcoin al Señor X.

- ✓ El Señor X le envía su clave pública a la Señora Y.
- ✓ Ésta agrega en la transacción la clave pública del Señor X junto con la cantidad a transferir.
- ✓ La Señora Y añadirá la transacción a la cadena de bloques.
- ✓ La Señora Y firma la transacción con su clave privada secreta. Declarando así que esas monedas que pertenecían a la Señora Y ahora pertenecen al Señor X.

Cualquiera que conozca la clave pública de ambos podrá ver que la Señora Y está de acuerdo en transferir una cantidad de Bitcoins al Señor X.

Cada firma lleva asociadas estas dos claves y la privada de cada firma es la única que se corresponde con la pública de la misma firma. Por eso es importante mantenerla en secreto porque si no otra persona podría firmar transacciones.

6.2 PREVIENE DEL DOBLE GASTO (10)

Esto es lo que garantizara que la Señora Y no pueda replicar la moneda y usarla en más de una transacción (esta es la mayor innovación detrás de Bitcoin):

- Los detalles de la transacción son enviadas y remitidas a todas las computadoras o a la mayor cantidad de computadoras posible.
- Éstas son añadidas a una cadena de bloques que crece constantemente y que se mantiene colectivamente por todos los computadores de la red de Bitcoin.
- Cada computadora de la red de Bitcoin posee una copia completa de este registro de bloques-transacciones.
- Para ser aceptados en la cadena, los bloques de transacciones deben ser válidos e incluir una prueba de trabajo.
- Los bloques son encadenados de forma que, si algún bloque es modificado, los bloques restantes tendrán que ser reconstruidos.
- Cuando aparecen múltiples continuaciones válidas en esta cadena, se aceptará sólo la rama más larga y consecuentemente se continuará extendiendo.

Así pues para poder confiar en que la transacción se llevará a cabo ésta debe de haber sido incluida en un bloque que forme parte de una larga cadena de bloques de rápido crecimiento (extendida con un significativo esfuerzo computacional). En ese momento la transacción habrá sido aceptada por la red de computadoras y será permanentemente registrada previniendo que la contraparte haga una segunda transacción con la misma moneda.

Ejemplo: El Señor X vende una colección de vinilos por 3 Bitcoins, la Señora Y está interesada y llegan al acuerdo de hacer la transacción en el siguiente bloque. Sin embargo en ese momento dos computadoras consiguen crear simultáneamente dos bloques, con lo cual la cadena se ve ramificada.

- ✓ La transacción será incluida en uno de los dos bloques que se han creado.
- ✓ Pero esperará hasta que se generen más bloques y ver por donde continúa la cadena para firmar la transacción con la clave privada.
- ✓ Si después de la creación vemos que la transacción se encuentra en la cadena que va a continuar se puede firmar sin ningún problema ya que se efectuará.

- ✓ En el caso de que la transacción se encuentre en la ramificación que no ha continuado con la cadena no se firmará ya que de lo contrario estos Bitcoins se perderían.

Así pues, en teoría, cualquiera podría intentar generar bloques falsos e intentar enviarle esos bloques a todo el mundo para gastar los Bitcoins en dos bloques a la vez. Sin embargo la anterior transacción y su firma ya ha sido anunciada y distribuida a un gran número de computadoras de la red Bitcoin y un bloque conteniéndola ya ha sido generado (de otro modo, el primer receptor de la moneda nunca hubiera recibido confirmación alguna). Además el proceso de generar un bloque válido está diseñado para tomar mucho tiempo, así que el que intente generar bloques falsos no podrá competir con el resto de computadores a la velocidad necesaria para generarlos.

Ejemplo: La Señora Y quiere realizar un fraude y hacer un doble gasto de la moneda. Si el Señor X no confía en la Señora Y tendrá que revisar los bloques que recibirá de terceras personas, que la Señora Y nunca podrá producir por sus propios medios, y alguno de esos nuevos bloques contendrá la transacción de la Señora Y lo que le dirá que ya gastó sus Bitcoins.

La única manera en la que la Señora Y puede borrar su pasada transacción es creando una cadena paralela que sea más larga que la cadena generada por todos, donde no exista registro alguno de su transacción, porque sólo la cadena más larga es aceptada por la red. Para seguir siendo larga, la cadena paralela de la Señora Y debe crecer más rápidamente que cualquier otra cadena, previniendo así que algún generador de bloques añada la transacción de la Señora Y a la cadena de transacciones. Para que esto sea posible, la Señora Y tiene que poseer de manera permanente bajo su control la mayoría de la potencia de CPU en la red, algo que asumimos que ninguna persona u organización puede hacer. Por lo tanto, mientras que las personas que controlen la mayoría de CPU no cooperen con la Señora Y, su transacción permanecerá registrada y le será imposible crear otra transacción con la misma moneda.

6.3 LAS TRANSACCIONES PERMITEN EL ANONIMATO (11)

Las "cuentas" Bitcoin no contienen en ellas el nombre de las personas y no necesariamente corresponden específicamente a individuos. Cada saldo simplemente se asocia con el par de claves pública-privada generado al azar y el dinero "pertenece" a cualquiera que pueda firmar con la clave privada cualquier transacción de esos fondos.

Las transacciones firmadas usando estas claves no incluyen los nombres de las personas que las realizan.

La dirección de Bitcoin del Señor X corresponde matemáticamente a una clave pública similar a esta:

1PC9aZC4hNX2rmmrt7uHTfYAS3hRbph4UN

Cada persona puede tener muchas direcciones como esta, cada una con su propio saldo, y esto puede hacer más difícil identificar qué persona tiene tal cantidad de dinero. Con el fin de proteger la privacidad cualquier usuario puede generar un nuevo par de claves pública-privada para cada transacción.

Sin embargo algunos criptógrafos del sector más duro con el Bitcoin opinan que no es tan fácil mantener el anonimato y que esto es uno de los puntos débiles del sistema. Su planteamiento es que se podría llegar a asociar una firma de Bitcoin con la dirección IP desde la cual se ha llevado a cabo la operación. Sin embargo aunque pudieran rastrear la dirección IP y asociarla a un nombre cualquier usuario puede realizar una operación desde una computadora ajena, sin saber ni siquiera si el titular asociado a esa dirección IP tiene acceso a esos fondos así que las supuestas autoridades no dispondrían de la certeza suficiente para congelar los fondos ligados a esa dirección Bitcoin. Además otra persona podría estar usando esa dirección IP generada por la computadora del usuario, podría estar usando las claves privadas que un día fueron del usuario, podría tratarse de una red pública o de un establecimiento, etc.

Si bien es cierto que cada usuario puede mantener el nivel de anonimato que desee ya que no se tiene porque se anónimo frente a todo el mundo, pueden elegir a quién revelar su identidad y en relación a qué direcciones Bitcoin.

Ninguna cuenta de Bitcoin se encuentra irremediablemente ligada a la identidad de un usuario, así aunque se pueda relacionar la transacción a un bloque y a una cuenta Bitcoin, no se podría relacionar a una identidad.

Podemos concluir que según lo que opinan los criptógrafos más extremistas y tras invertir grandes cantidades de recursos tecnológicos y humanos como mucho será posible probar que alguien que no desea revelar su identidad tuvo quizás, alguna vez, Bitcoin bajo su control, sin saber cuántas otras direcciones posee y sin saber si esos Bitcoin siguen en su poder o han sido transferidos, etc. y sin poder congelar ni confiscar esos fondos, ni decidir a qué fines pueden ser destinados.

Bitcoin impide los abusos de poder que son perpetrados de una manera extraordinariamente sencilla y económica por medio del sistema bancario semi-estatal. Nada puede hacerse para eliminar el Bitcoin ya que su funcionamiento depende de la propia infraestructura de telecomunicaciones que hace posible internet. Por eso, si una institución reguladora quisiese destruir el Bitcoin, tendría que destruir todo el sistema para ser eliminado como sucede con los virus informáticos.

Nadie puede decir que el Bitcoin es más vulnerable a ataques que el euro, ya que el Bitcoin es digital y no está sujeto a control, para lo bueno y para lo malo. Es cierto que se puede usar para comprar drogas, es lo que tiene una herramienta que puede ser anónima, a internet le pasó lo mismo en sus inicios, era malo porque personas lo usaban para comunicarse secretamente con mala fe, todos podemos ver cómo ha acabado internet.

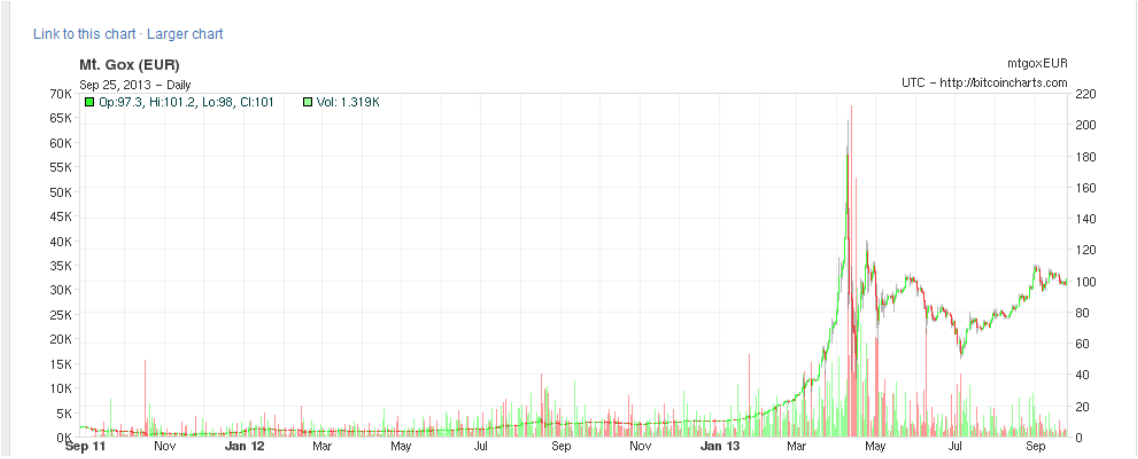
La Bitcoin Foundation, creada en 2012, tiene entre uno de sus objetivos fundamentales el mantener una economía que no dependa de la política, que sea abierta e independiente.

La forma más habitual de proteger los Bitcoins es realizar varias copias idénticas del fichero *wallet.dat*, cifradas con una contraseña fuerte, y guardarlas físicamente en varios soportes USB y en la nube. Algunos usuarios más avanzados prefieren la aplicación de esteganografía (oculta mensajes u objetos dentro de otros), o incluso generar la clave privada únicamente a partir de una frase memorizada, sin necesidad de ningún soporte físico.

Otros optan simplemente por imprimir en papel la clave privada en formato numérico o en QR (Quick Response code "código de respuesta rápida", es como un código de barras que aporta información) y guardarla en un lugar seguro.

7. COTIZACIÓN DEL BITCOIN

Gráfico 7.1: Evolución cotización del Bitcoin septiembre 2011 – septiembre 2013



Fuente: http://bitcoincharts.com/

Como se puede observar en el gráfico 7.1 el valor en euros por Bitcoin se mantenía con cierta estabilidad y valores muy bajos hasta 2013 cuando empezó a aumentar y fue en abril cuando se produjo la gran subida donde se alcanzaron los picos que podemos observar en los gráficos. Este hecho coincidió con el momento en que se empezó a difundir información de esta moneda a nivel mundial y todos los medios de comunicación se hicieron eco de ello.

Gráfico 7.2: Ampliación de la "burbuja" de abril 2013

Fuente: http://bitcoincharts.com/

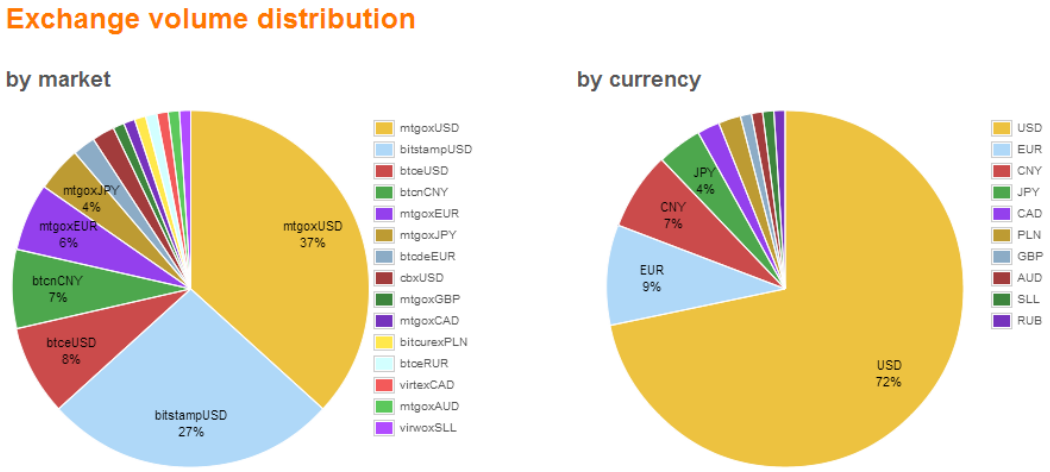
Si observamos la evolución que se ha producido después de los picos alcanzados en abril en el gráfico 7.2, podemos observar que se está menteniendo el Bitcoin en una banda entre los 120€/Bitcoin y los 60€/Bitcoin, va oscilando con mucha volatilidad pero no ha vuelto a tener ninguna bajada o subida considerable como las ocurridas en abril.

Gráfico 7.3: Análisis volatilidad septiembre 2013

Fuente: http://bitcoincharts.com/

Si observamos sólo el mes de septiembre (gráfico 7.3) podemos ver que se está manteniendo en torno a los 100€/Bitcoin y la banda de Bollinger (las dos curvas que envuelven el gráfico de precios) nos muestra la volatilidad que puede tener el precio del Bitcoin.

Gráfico 7.4: Distribución del cambio de divisas



Fuente: http://bitcoincharts.com/

En el gráfico 7.4 podemos observar como el cambio de divisas está localizado en más del 70% entre dos casas de cambio, MTGOX y BitstampUSD. Mientras que estás operaciones en un 72% son en dólares, seguidas muy de lejos por los euros en un 9%.

8. APLICACIONES (12)

8.1 BITCOIN PARA PERSONAS

Bitcoin es la forma más sencilla de cambiar el dinero a un costo muy bajo.

- ✓ Pagos a través del móvil

  Es una manera fácil de realizar pagos. Tan sólo se tienen que llevar a cabo dos pasos: escanear y pagar. Es decir, a través de un código QR y con la aplicación de la cartera instalada en el smartphone y que éste sea escaneado por la contraparte o bien a través de la tecnología NFC que permite que con tan sólo acercar dos smartphones se transfiera información. No hace falta tarjeta, escribir un número de identificación o firmar cualquier cosa.

- ✓ Realizar transacciones de manera segura

  Como anteriormente hemos comentado el sistema de criptografía utiliza seguridad de nivel militar. Si no se poseen las claves nadie puede hacer uso de la billetera, así que si el usuario sigue los pasos necesarios para proteger el monedero los fraudes se evitarán.

- ✓ Funcionalidad

  Es un sistema que funciona en todas partes y en cualquier momento, como ocurre con el correo electrónico, no es necesario utilizar el mismo software o los mismo proveedores de servicio. Cada usuario puede utilizar sus servicios favoritos sin que haya problemas de compatibilidad ya que todos ellos usan una tecnología abierta. Un ejemplo análogo sería a la hora de hacer una transacción de una entidad bancaria a otra diferente, en este caso casi todas cobran una cantidad en concepto de comisión.

- ✓ Pagos internacionales

  Su uso se ha visto incrementado para hacer pagos internacionales ya que se hacen de una manera rápida, en 10 minutos, es una buena solución para los inmigrantes que quieren enviar dinero a sus familiares a otro país. No existe un banco que retrase el proceso, comisiones muy elevadas o que congelen la transferencia.

- ✓ Pagos gratuitos

  Salvo en casos especiales como cuando los pagos son diminutos, Bitcoin permite enviar y recibir pagos de forma gratuita, es decir, no existe ningún tipo de cuota que se deba satisfacer para llevar a cabo el proceso. Sin embargo como hemos comentado anteriormente se puede pagar una pequeña comisión para asegurar que la transacción esté presente en el siguiente bloque, comisión que recibirá el creador del bloque.

- ✓ Pagos anónimos

  Bitcoin aporta a los usuarios de esta red el anonimato que está presente en casi todas nuestras compras diarias donde no se identifica al usuario. Permite desde comprar servicios hasta hacer donaciones sin tener que dar los datos del usuario.

- ✓ Fideicomiso

  Si realizamos compras de particular a particular, como por ejemplo artículos de segunda mano, es posible usar un servicio de fideicomiso que muchas páginas especializadas en venta de segunda mano con bitcoins ya ofrecen. Nosotros realizamos el pago a la página y esta no lo procesa al vendedor hasta que el producto ha llegado a su destino. Una de las páginas que ofrece servicio de fideicomiso es la página de subastas y venta de segunda mano Bitmit (En inglés se llama "escrow").

8.2 BITCOIN PARA EMPRESAS

Bitcoin es una forma muy segura y de bajo costo para gestionar pagos por las siguientes razones:

- ✓ Tarifas bajas

  La alta seguridad criptográfica de Bitcoin le permite procesar las transacciones de una manera muy eficiente y a bajo coste ya que en la mayoría de los casos la comisión es cero.

- ✓ Protección contra el fraude de pago y devolución de cargos

  Los negocios que aceptan pagos en línea a través de tarjetas de crédito o PayPal conocen el problema de los pagos que luego son revertidos por el remitente porque le habían hackeado sus cuentas o porque no se realizó la entrega del producto. La única manera en la que las empresas pueden defenderse contra este tipo de prácticas es realizar un análisis de riesgos complejos y aumentar los precios para cubrir pérdidas. Sin embargo los pagos con Bitcoin son irreversibles y las carteras se pueden mantener de forma muy segura de tal forma que los costes asociados a un robo no recaen sobre los comerciantes.

- ✓ Rapidez en los pagos internacionales

  Los Bitcoins no tienen ninguna ubicación física real, así que se pueden transferir tantos como se desee a cualquier lugar sin límites, demoras o costes excesivos. A diferencia de lo que ocurre con los bancos para las operaciones internacionales que hacen esperar tres días hábiles, en este sistema no existen intermediarios que ralenticen las operaciones.

- ✓ Estándar PCI

  Este estándar consiste en una guía que ayuda a las organizaciones que procesan, almacenan y/o transmiten datos para prevenirles contra los fraudes que involucran tarjetas de pago de débito y de crédito. Así que la aceptación de las tarjetas de crédito/débito en línea requiere, por lo general, extensas comprobaciones de seguridad a fin de cumplir con este estándar. Sin duda alguna es una buena forma para proteger las tarjetas de crédito pero la seguridad

de Bitcoin está construida de tal manera que hacen que este enfoque quede obsoleto ya que los pagos están garantizados por la red, no a su cargo, con lo cual no debe cumplimentar este estándar.

- ✓ Posicionamiento

  El simple hecho de aceptar pagos con esta nueva moneda permite conseguir nuevos clientes y dar a su negocio cierta visibilidad. Aceptar una nueva forma de pago siempre ha demostrado ser una práctica inteligente para los negocios en línea como ya ocurriera en su día con el sistema PayPal por ejemplo.

- ✓ Multi-firma

  Bitcoin también incluye una característica que no es aún muy conocida, que permite que los Bitcoins puedan ser utilizados sólo si un subconjunto de un grupo de personas firman la misma transacción (llamado transacciones "n de m"). Este es el equivalente de las firmas mancomunadas de control que usan los bancos hoy en día. Se trata de generar una dirección que requiera la combinación de varias claves privadas. Como hemos comentado en el apartado 5.4 Cartera se necesitaría más de una clave privada para firmar las transacciones y estas pueden estar guardadas en dispositivos diferentes.

- ✓ Transparencia contable

  Muchas organizaciones están obligadas a presentar los documentos contables sobre sus actividades, y a la adopción de buenas prácticas de transparencia. Usando Bitcoin se ofrece el más alto nivel de transparencia ya que su balance y sus transacciones son públicos para sus miembros si se los mantiene al tanto de sus direcciones de Bitcoin.

- ✓ Para los sectores más regulados

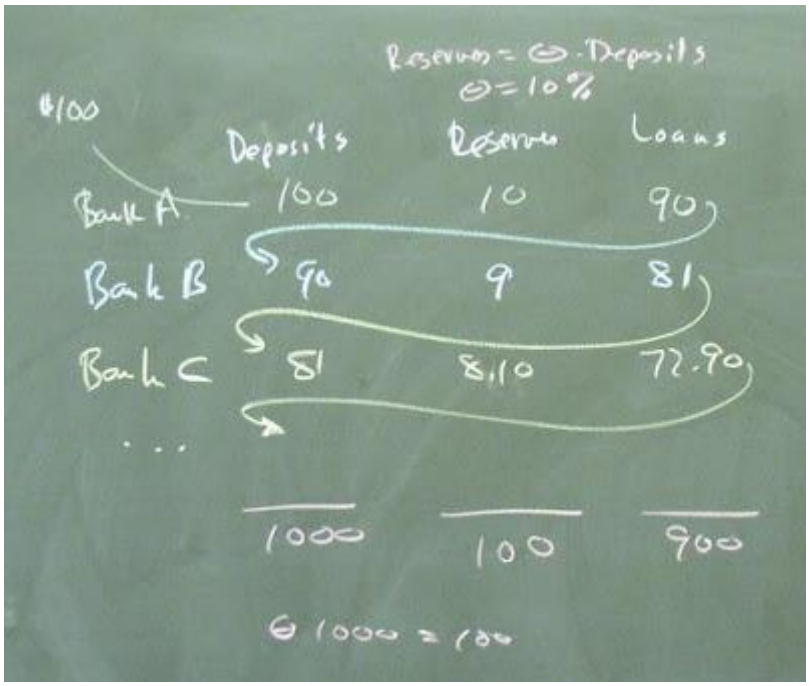
  El ámbito internacional y el hecho que los usuarios pueden comerciar con un cierto anonimato, ha hecho posible que se abra paso en sectores cada vez más regulados, como apuestas online y partidas de póker.

8.3 BITCOIN PARA LOS BANCOS

Existe diferencias entre las monedas nacionales y los Bitcoin como se ha analizado a lo largo del trabajo

Actualmente, prácticamente la totalidad de las divisas nacionales como el euro o el dólar es dinero fiduciario (que se basa en la confianza de la comunidad y no está respaldado por un material precioso). Es decir, su valor real es mucho mayor que su coste de producción, y es emitido por los bancos centrales mediante la creación de deuda que se multiplica a través de los bancos comerciales y el sistema de reserva fraccionaria.

Gráfico 8.1: Sistema de Banca con reserva fraccionaria



Fuente: http://es.globedia.com/sistema-bancario-sociedad-libre

En contraposición al dinero fiduciario, Bitcoin utiliza un sistema de prueba de trabajo que simula el minado de materias primas hasta el punto de que el precio de los Bitcoins es igual al coste marginal de producción (el incremento del coste total que supone la producción adicional de una unidad de un determinado bien) ya que los mineros están continuamente compitiendo por ser los más eficientes. Los mineros dedican sus recursos de tiempo, energía, procesamiento y amortización de máquina para resolver un desafío criptográfico complejo.

Por estas razones y que su escasez no es natural sino generada a través de un algoritmo matemático, el economista George Selgin califica a Bitcoin como cuasi-materia prima (*quasi-commodity money*).

Por otra parte, los Bitcoins poseen todas las características necesarias para ser considerado dinero (13). Es altamente divisible (hasta ocho decimales), denso en valor (una dirección puede contener millones de euros), inmediatamente reconocible con el software adecuado y fungible (cada unidad está valorada de la misma forma). Asimismo, la posesión de la clave privada es control. Las claves privadas pueden guardarse en una cartera electrónica o generarse a partir de una frase más o menos larga, que es suficiente con memorizarla. Esta última característica, unida al hecho de que la dirección Bitcoin es un pseudónimo y no refleja la identidad real de su propietario, hace que los Bitcoins sean difíciles de confiscar.

Los posibles escenarios de fracaso para Bitcoin son una depreciación de la moneda, una disminución de los usuarios, o una campaña gubernamental global en contra del software.

Como el núcleo del protocolo Bitcoin no cifra ningún tipo de información, todas las transacciones son públicas y cualquier observador externo puede analizar en cualquier momento su contenido, el origen y el destino de todos los mensajes. Esta característica contrasta con el modelo bancario tradicional que oculta las transacciones del escrutinio público.

8.4 QUÉ SE PUEDE COMPRAR (12)

- ✓ Coches
- ✓ Videojuegos
- ✓ Casino
- ✓ Electrónica
- ✓ Fotografía
- ✓ Videoconsolas
- ✓ Flores
- ✓ Dispositivos ecológicos
- ✓ Oro
- ✓ Plata

- ✓ Hoteles
- ✓ Comida (Domino's Pizza)
- ✓ Software
- ✓ Descargas
- ✓ Blogs (Wordprees)
- ✓ Servidores, dominios, hosting y hardware
- ✓ Juguetes
- ✓ Ropa
- ✓ Libros
- ✓ Películas
- ✓ Música
- ✓ Salud
- ✓ Deporte
- ✓ Telecomunicaciones
- ✓ Limpieza y hogar
- ✓ Joyas
- ✓ Arte
- ✓ Mascotas
- ✓ Servicios
- ✓ Suscripciones
- ✓ Compras online de todo tipo

Así que a día de hoy se puede comprar prácticamente de todo con esta moneda.

9. OPORTUNIDADES DE FUTURO

Actualmente cuesta mucho encontrar activos de calidad, activos que sean seguros donde depositar los ahorros. Existe incertidumbre sobre el euro, sobre el dólar, sobre el yen, sobre la libra, etc que se ven afectadas por conflictos como el de Siria, situaciones como la de Grecia (al euro), etc. Existen pocas monedas que inspiren confianza así como pocas empresas que tengan una perspectiva optimista o expectativas positivas en el futuro, la incertidumbre es muy elevada y muchos inversores optan por depositar parte de sus ahorros en Bitcoin, aunque se trate de una moneda virtual.

Realmente el Bitcoin no es una moneda refugio o valor de inversión, ésta ha sido diseñada para la transacción de bienes y servicios en internet, es decir, para comprar y

vender, no para especular (15) y (19). Pero esto no quita que haya habido usuarios que se han aprovechado de la situación para comprar grandes volúmenes y así animar a nuevos inversores sin conocimientos para especular con el Bitcoin.

Esta especulación puede resultar exitosa (o no) porque el volumen monetario de Bitcoins ahora mismo es pequeño y la volatilidad de la moneda es muy alta. Es decir, pocos movimientos de compra provocan grandes movimientos en su cotización, pero cuando se convierta en una moneda de utilización global su variabilidad será mínima. Esto no se puede hacer con monedas como el euro o el dólar ya que aunque exista incertidumbre, su volatilidad es muy poca.

Es decir con esta variabilidad se puede especular pero de momento, y hasta que más personas lo utilicen (que llevará años), no se pueden establecer salarios o precios de compra y venta de productos y servicios.

Pero realmente el Bitcoin no sirve para la inversión, el Bitcoin se ha creado para transacciones de bienes y servicios, este es su único objetivo. El problema que debido a la desinformación de muchas personas hay otros que lo utilizan para especular.

Basándonos en lo que Keynes llamaba depósito de valor de una moneda, si sirve para transacciones de bienes y servicios el Bitcoin debería servir también como inversión, pero para ser considerado depósito de valor se requiere estabilidad de precios y como hemos comentado anteriormente esto se conseguirá cuando millones de personas usen de manera cotidiana Bitcoin como medio de pago.

Como hemos comentado en el apartado 8.2 Bitcoin para empresas es una oportunidad para que las empresas innoven y se posicionen dándose a conocer al aceptar estos sistemas de pagos.

A día de hoy si lo que se quiere es ganar dinero con el Bitcoin la manera de hacerlo es a través de la minería (se están pagando 25Bitcoins por bloque generado) así que si se realiza una inversión en buenas computadoras, GPUs, Asics, etc. para hacer minería se puede obtener muchos beneficios. Como toda inversión tiene su riesgo y habría que realizar un estudio del coste de los ordenadores a comprar, del gasto energético que supondría mensualmente, del tiempo que habría que dedicar, etc. De todas maneras existen páginas donde cualquiera puede contribuir a la creación de bloques (mining

pools) donde el premio es repartido entre todos los que aportan su potencia del ordenador para la red Bitcoin como hemos comentado anteriormente. Esto puede permitir ganar una pequeña cantidad mensualmente sin gastar prácticamente energía.

Puede ser una apertura mundial para que en todos los países sea utilizado, incluso en aquellos en los que existen determinadas barreras. Como ocurre con la plataforma WordPress que acepta pagos en Bitcoins en todo el mundo, incluyendo a los más de 60 países bloqueados por PayPal, para evitar que blogueros de Haití, Etiopía o Kenia tengan un acceso limitado a la blogosfera por "problemas en los pagos que quedan fuera de su control".

Al estar desregulado y poder conseguir el anonimato es una oportunidad para conceder donaciones a plataformas que intentan mantenernos informados de hechos conflictivos ya sean presentes o pasados como Wikileaks, que tras sufrir un bloqueo por parte de los procesadores de pago electrónico Visa, MasterCard y PayPal, solicitó asistencia en Bitcoins. Por supuesto también es muy práctico para que las ONGs reciban donaciones ya que mantiene el anonimato del emisor de la donación.

Los intercambios a divisas nacionales se llevan a cabo a través de oficinas por internet y de persona a persona. En Estados Unidos, en varios de los principales bancos así como en los centros comerciales Walmart y 7-Eleven entre otros, admiten depósitos de dinero en efectivo para convertir a Bitcoins, y también en países como Brasil y Rusia a través de varias entidades.

10. DESREGULARIZACIÓN

El Bitcoin apenas se ha regulado, pero los supervisores como el BCE están atentos a sus movimientos tal y como afirmaron en un informe de 2012 que el sistema Bitcoin sólo suponía un riesgo para los agentes que participaran en él. El departamento del Tesoro de EEUU reconoce que las divisas virtuales no están bajo su regulación pero si las plataformas de intercambio.

En China en 2009 ya se prohibió comerciar con Q-coins, una moneda que se compraba con saldo prepago para comprar servicios prestados por la compañía Tencet, pero que acabó siendo aceptada para pagos entre particulares.

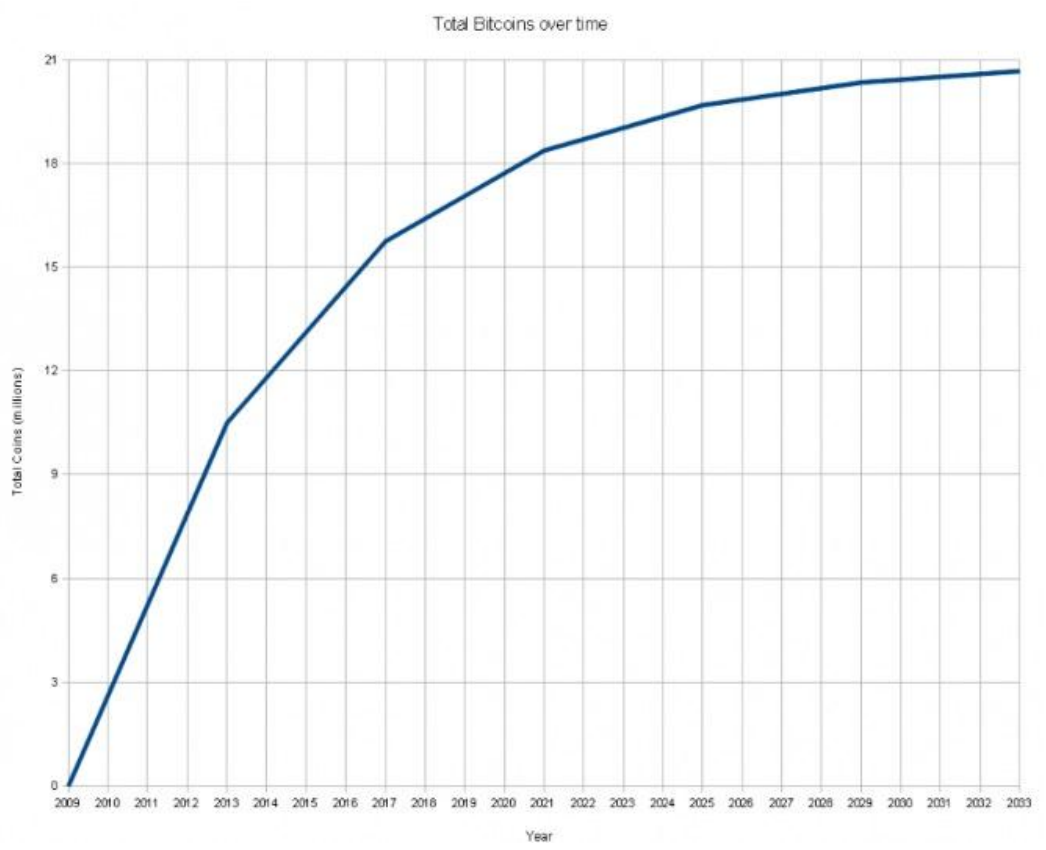
La principal diferencia que tiene el Bitcoin con cualquier moneda del mundo es que no hay un país que establezca su existencia, no hay un Banco Central responsable de su emisión y regulación, no hay un órgano que disponga si se devalúa o se revalúa frente a otras monedas, se basa en la confianza de los usuarios de la red Bitcoin para realizar transacciones y operaciones con esta moneda (14).

El dinero aceptado en la sociedad tiene este componente regulatorio controlado por un organismo o entidad pero a la vez tiene un valor intrínseco de confianza otorgado por la sociedad que lo utiliza, en el caso del Bitcoin solo se basa en este valor intrínseco.

A diferencia del resto de monedas del mundo, la oferta de bitcoins no está controlada por autoridades sino por la casualidad ligada a complejos protocolos informáticos. Esto lo podríamos comparar con lo que pasaba con el oro cuando era utilizado como dinero, la oferta del mismo dependía de si se encontraba una mina nueva o se asaltaba un barco cargado de oro procedente de otro país. Por todos es conocido que las reservas de oro un día se acabarán, lo mismo ocurre con los Bitcoin, que los problemas son más complejos conforme se solucionan los anteriores, es decir, la dificultad del mining para conseguir Bitcoins es creciente y el objetivo de los creadores es que se llegue un día (en 2040 cuando se alcancen los 21 millones) que la dificultad de los problemas matemáticos sean tan complejos que no se puedan crear más Bitcoin.

Como pasa con el oro, a la larga la oferta de Bitcoins va a ser constante por los siglos de los siglos. De hecho se espera que la oferta de Bitcoins siga el camino del gráfico 10.1. En 2013 hay unos 11 millones de monedas en circulación, en 10 años se calcula que está cantidad se doblará más o menos y de ahí hasta la creación de los 21 millones exactos se mantendrá casi constante

Gráfico 10.1: Expectativas de evolución de la oferta de Bitcoin.



Fuente: http://goo.gl/83I49m

Esta desregularización, como hemos dicho, hace que se base en la confianza que los usuarios le dan a este sistema de pagos y como no existe ningún banco que haga de intermediario las comisiones por transferencias de dinero son mínimas (en el caso de que existan). Los usuarios no tienen que dar cuenta de nada a nadie e incluso si se esfuerza puede conseguir el anonimato. Se convierte en un sistema más libre, donde la fiabilidad de una operación viene dada por las partes, es decir, si por ejemplo una empresa como Samsung, Starbucks, Apple, etc. comienza a aceptar pagos en Bitcoin a sus clientes y a otros usuarios les dará confianza y una casi completa fiabilidad. También es cierto que se usa para vender drogas y blanquear dinero que serían unos de los puntos a solucionar, permitiendo identificar a aquellos que llevan a cabo actividades ilícitas.

Bitcoin es una moneda que se auto-regula y representa el estado real de su economía, pues nadie puede hacer que cambie de valor de manera artificial o forzada. Por supuesto esto a los bancos y autoridades centrales no les interesa.

11. EL BITCOIN ¿UNA BURBUJA ECONÓMICA? (16)

En abril de 2013 se produjo una subida espectacular de la cotización del Bitcoin que en 4 meses creció un 1.655% lo que hizo pensar que se trataba de una burbuja donde los inversores que llegan más tarde pagarían los rendimientos de los que llegaron primero. Muchos analistas apuntaron que podría convertirse en un esquema piramidal. Sin embargo, hoy por hoy, se parece más a una materia prima que a cualquier tipo de dinero, aunque desde el BCE apuntan que el Bitcoin se parece muchísimo al dinero en efectivo.

Muchos economistas tildan de burbuja económica al sistema de Bitcoin afirmando que el valor de Bitcoin tiene que reventar, incluso diarios como Financial Times han tenido titulares tan rotundos como “Bitcoin bubble grows and grows”.

Entre los detractores del Bitcoin hay que destacar a los economistas austriacos que no terminan de encajar los Bitcoin dentro del teorema regresivo de Mises (teorema que pone de manifiesto que el dinero se demanda hoy por la experiencia histórica de lo que se ha podido comprar últimamente con ese dinero) y los partidarios del patrón oro que lo ven como una potencial competencia.

Normalmente, cuando se produce un aumento de la demanda de los activos monetarios su precio de equilibrio aumenta, es decir, cuantas más personas deseen atesorar Bitcoins más se apreciará frente al resto de activos monetarios (tipo de cambio: apreciación) y no monetarios (precio de los activos: deflación). Pero esto no se debe interpretar como que cualquier aumento de demanda de un activo monetario lo aleja del territorio burbuja porque si el aumento de la demanda tiene un componente especulativo la probabilidad de que el precio futuro del Bitcoin se derrumbe puede ser creciente. Podríamos compararlo con la burbuja española, un aumento de la demanda de inversión de viviendas en 2007 no hubiese reducido la burbuja inmobiliaria sino que la hubiera incrementado.

Entonces para que el aumento de precio no se deba simplemente a una especulación se puede entender que los especuladores pueden interpretar que la información sobre Bitcoins se va a seguir extendiendo y que, al conocerla más, cada vez más gente querrá introducirlas en su patrimonio y por eso su precio futuro será superior al actual de tal manera que esta demanda especuladora estabilice el Bitcoin. Lo que está claro es que hasta que no se estabilice su precio no se adoptará como moneda independiente al dólar o euro.

En un futuro, si se estabiliza (que puede ser a un tipo de cambio muy superior al actual), cada vez será más sencillo mantener la contabilidad de una parte de nuestro patrimonio en Bitcoins, es decir, cuando muchos agentes participen en transacciones a través de Bitcoins se podrá obtener una parte de ingresos en Bitcoins y efectuar una parte de gastos con ellos sin tener un riesgo cambiario.

Una vez estabilizada puede derrumbarse pero no porque existiera una burbuja sino porque la demanda ha caído por situaciones exógenas a las características propias del activo y su precio.

En definitiva, la mayor o menor demanda monetaria de un activo modifica su valor de equilibrio a largo plazo, de tal forma que en épocas en las que la demanda no sufra cambios muy bruscos se podrá predecir de manera más o menos aceptable su valor, por el contrario cuando la demanda es inestable y caótica la volatilidad de los tipos de cambio se dispara. A día de hoy la volatilidad es muy elevada dado que el Bitcoin se está dando a conocer, está en sus primeros pasos y cada vez más gente puede estar incorporándola en sus patrimonios, con lo cual los análisis de valores de la divisa, que deben basarse en un conocimiento y acceso a toda la información relevante, no son concluyentes por encontrarse en esta fase, donde los agentes tienen hoy más información de la que tenían ayer. Así que el problema radica en saber si los inversores que compran Bitcoin hoy las liquidarán de manera masiva en el futuro o las adoptarán realmente como una divisa.

Podemos concluir que si prosigue con su avance de monetización y llega a completarse, siempre y cuando no haya nada que lo imposibilite, el precio futuro del Bitcoin será muy superior al actual, es decir, Bitcoin puede seguir subiendo sosteniblemente de

precio sin que se trate de una burbuja. Nos podemos preguntar si su futuro es incierto, pero ello no determina que se trate de una burbuja. Además si este proceso de monetización se produce en un futuro puede llegar a ser un sustituto real del dinero físico, siempre y cuando la tecnología siga avanzando como hasta ahora (17).

En este proceso se pueden observar unos riesgos inherentes al Bitcoin:

- ✓ Riesgo de que no llegue a desarrollarse como moneda (el más importante de todos).
- ✓ Riesgo de ilegalización (En el caso de la ilegalización no está claro que sea un riesgo muy elevado ya que Bitcoin está pensada precisamente para ser intercambiado al margen del gobierno).
- ✓ En cuanto a riesgo de robos está muy protegido con el sistema de claves, siempre y cuando el usuario sea cauto respecto a su conservación y uso.

En el caso de que alguno de estos riesgos se materializase su precio volvería a ser cero siendo cualquier precio actual una burbuja.

Como curiosidad podemos apuntar que la popularidad de búsquedas en google ha ido asociada casi milimétricamente con el aumento del precio del Bitcoin y que en países como Alemania ya reconocen el Bitcoin como moneda. Alemania, al igual que EEUU, estudia de qué forma tributarán las transacciones realizadas por particulares en Bitcoins. Al contrario que las autoridades alemanas, el banco central tailandés declaró en julio de 2012 ilegal comerciar en bitcoins, usarlos para vender bienes o servicios en el país o introducirlos o sacarlos de Tailandia.

12. ALTERNATIVAS (ALT-COINS) (18)

Existen diversas alternativas al Bitcoin, aunque ninguna genera tanta confianza ante los usuarios como ocurre con el Bitcoin. Estas alternativas se llaman alt-coins. Quizás algunas alt-coins lleguen a ser importantes en el futuro cuando se generalicen las criptomonedas ya que por el momento no cubren alguna necesidad insatisfecha y lo único que hacen es confundir a los interesados que ya tiene suficientes dificultades para entender los Bitcoin así como desviar el talento del capital humano hacia otras alt-coins.

Ventajas del Bitcoins respecto de las alt-coins:

- ✓ Fist mover advantage: es decir, la ventaja del pionero, aunque esto no implica un éxito asegurado frente a la competencia siempre implica una enorme ventaja y mientras siga siendo así de dinámico no se verá superado por los competidores.
- ✓ El efecto de red: es decir, se trata de una moneda y las monedas resultan más útiles cuantas más personas las utilizan de tal forma que en su mayoría quienes eligen a Bitcoin lo hacen porque muchos otros lo han elegido antes.
- ✓ Poder computacional: aunque el código de otras alt-coins sea casi igual al de Bitcoin la seguridad del sistema dependerá del poder computacional que aporten los mineros a la red. Sin un apoyo de mineros bien incentivados ningún proyecto tendrá posibilidades de hacerle la competencia al sistema Bitcoin.
- ✓ Ecosistema: alrededor de Bitcoin existe un amplio conjunto de programadores, comerciantes, consumidores, emprendedores, mineros, operadores, etc. difícil de superar por otras alt-coins.
- ✓ Liquidez: entre dos monedas los usuarios siempre preferirán a la más líquida y a la más fácilmente intercambiable en todo momento por cualquier activo.
- ✓ Confianza: muchos de los usuarios de Bitcoin están huyendo de sistemas monetarios que basan su confianza en determinadas instituciones humanas. Están eligiendo antes la certeza de las matemáticas que las promesas de un gobierno o autoridades monetarias.
- ✓ Comodidad: para los que han empezado a utilizar Bitcoin pasarse a otra alt-coin siendo que han comenzado a entender el funcionamiento de Bitcoin les desincentiva.

Alternativas:

- ✓ Litecoins (usa un puzle matemático que no se puede resolver con las GPUs o CPUs, así que la actividad de minado no recae sobre los que tienen equipos más caros sino que pueden competir un mayor número de mineros).
- ✓ PPCoin (pretende eliminar la minería convencional repartiendo en una especie de lotería las PPcoins entre los usuarios donde las probabilidades de ganar vienen dadas por cuantas se poseen).
- ✓ Quantum-coins (monedas que se generarán a través de ordenadores cuánticos).

- ✓ En el anexo se encuentran otras alt-coins como: Eathercoin, Digitalcoin, Worldcoin, Phenixcoin, etc.

También existen monedas en los mundos virtuales de videojuegos de rol, dinero que sirve para comprar artículos dentro del videojuego y en los más populares, aunque está prohibido, el dinero del videojuego se cambia por dinero real. Así mismo están las propiamente creadas para el ecommerce como Facebook Credit, las Amazon Coins y Apple, después de su rechazo a aplicaciones de cartera de Bitcoins y haber perdido clientes, podría desarrollar en un futuro iMoney. Estas monedas las compra el usuario con dinero real y las usa para adquirir bienes pero sólo en dichas plataformas.

Según el economista George Selgin la competencia simplemente aumenta las posibilidades de que alguna criptomoneda tenga éxito (20).

13. CONCLUSIONES

En el presente trabajo hemos estudiado la naturaleza del Bitcoin. Partiendo de su misterioso origen hemos discutido las características principales de esta moneda, en especial su naturaleza asociada a la computación, así como su especial estructura criptográfica. El modo con el que las operaciones comerciales tienen lugar mediante el Bitcoin ha sido objeto de estudio a lo largo del presente trabajo. La generación de la moneda (minería) y su extendido uso comercial, con particular énfasis en su naturaleza peer to peer y la imposibilidad del doble uso, han sido analizados ampliamente. Las ventajas y desventajas de esta nueva moneda han sido descritas y sus fuertes fluctuaciones comentadas en profundidad, en especial su comportamiento como posible burbuja económica. Analizadas las virtudes y defectos de esta nueva manera de abordar el comercio y las finanzas, nuestra conclusión es positiva. Creemos, apoyándonos en nuestro estudio, que el uso de los Bitcoins es provechoso fundamentalmente para el comercio ya que éste tiene que ser su principal fin, aunque si sigue con su proceso de monetización cabe esperar a largo plazo, que aumente su valor, por lo que debería formar parte de una cartera de valores diversificada. Por lo que se refiere al comercio, el uso del Bitcoin en las transacciones comerciales se está extendiendo a gran ritmo, casi exponencialmente, y el número de comercios que aceptan esta moneda crece día a día. Dada su conexión con la informática y la encriptación y la amplia aceptación que está adquiriendo en conexión con la red, creemos que esta moneda posee un gran potencial y requerirá de más cuidadosos y amplios estudios que dejamos para un trabajo futuro.

Agradecimientos en primer lugar a mi tutora, la profesora Begoña Gutiérrez Nieto, por su paciencia, su continua ayuda y su disposición a atender todas mis dudas. En segundo lugar a los miembros del BIFI, Yamir Moreno, Francisco Sanz y Alejandro Rivero por las continuas charlas que me han permitido introducirme en este tema tan complejo y por supuesto a mi familia y amigos que me han aguantado durante la realización de este trabajo.

14. Fuentes

(1) 1-Wei Dai. "b-money", http://www.weidai.com/bmoney.txt

(2) Satoshi Nakamoto (1 de noviembre de 2008). "Bitcoin: A Peer-to-Peer Electronic Cash System", http://www.bitcoin.org/bitcoin.pdf

(3) Joshua Davis. The crypto-currency: Bitcoin and its mysterious inventor. The New Yorker, October 10, 2011.

(4) http://blockexplorer.com/

(5) Una referencia general: https://en.bitcoin.it/wiki/Main_Page

(6) Referencia de android: http://goo.gl/CZd7VV

(7) Jan A. Bergstra, Karl de Leeuw. Questions related to Bitcoin and other Informational Money, (Submitted on 25 May 2013). http://arxiv.org/abs/1305.5956

(8) Artus Krohn-Grimberghe Christoph Sorge. Practical Aspects of the Bitcoin System http://arxiv.org/abs/1308.6760

(9) Barber, Simon; Boyen, Xavier; Shi, Elaine and Uzun, Esrin (2012). "Bitter to Better — how to make Bitcoin a better currency". Financial Cryptography and Data Security. Lecture Notes in Computer Science (Springer) 7397 pp 399-414

(10) Matthias Herrmann. Implementation, evaluation, and detection of a double-spend attack on Bitcoin. MSc Thesis, ETH Zürich (2012)

(11) Reid, F., & Harrigan, M. (2013). An Analysis of Anonymity in the Bitcoin System. In Security and Privacy in Social Networks.New York: Springer

(12) Jung-San Lee, Kun-Shian Lin. A robust e-commerce service: Light-weight secure mail-order mechanism. Electronic Commerce Research and Applications, Volume 11, Issue 4, July–August 2012, Pages 388-396

(13) Reuben Grinberg. Bitcoin: an alternative digital currency. Hastings Sci. and Tech.Law Journal, 159–208 (2012).

(14) Does modern banking lead to money privatization? Original Research Article International Economics, Volume 133, May 2013, Pages 50-71 Thomas Grjebine

(15) Dániel Kondor, Máton Pósfai, István Csabai, Gábor Vattay. Do the rich get richer? An empirical analysis of the BitCoin transaction network, (Submitted on 18 Aug 2013). http://arxiv.org/abs/1308.3892

(16)A. Hüsler, D. Sornette, C.H. Hommes. Super-exponential bubbles in lab experiments: Evidence for anchoring over-optimistic expectations on price. Journal of Economic Behavior & Organization, Volume 92, August 2013, Pages 304-316

(17)Ron, D. and Shamir, A. (2012). Quantitative Analysis of the Full Bitcoin Transaction Graph.
http://eprint.iacr.org/2012/584

(18) Jan A. Bergstra, Karl de Leeuw. Bitcoin and Beyond: Exclusively Informational Monies (Submitted on 17 Apr 2013 (v1), last revised 12 May 2013 (this version, v2))
http://arxiv.org/abs/1304.4758

(19)Marie Brière, Kim Oosterlinck and Ariane Szafarz. Virtual Currency, Tangible Return: Portfolio Diversification with Bitcoins. Université Libre de Bruxelles - Solvay Brussels School of Economics and Management Centre Emile Bernheim. CEB Working Paper N° 13/031 september 2013.
http://ideas.repec.org/p/sol/wpaper/2013-149159.html

(20) George Selgin. Synthetic Commodity Money. Department of Economics, University of Georgia
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2000118

15. Anexos:

I. **Comercios en castellano.** Fuente: https://es.bitcoin.it/wiki/Comercio

Todo el Mundo

- Bitcoin2CDKey.com: Venta de CD Keys para steam, origin, games for windows live, ubisoft y muchos más. También vendemos servicio de templates para páginas de facebook y video intros para tus videos.

- ComprarKey.com: Venta de CD Keys para steam, origin, games for windows live, ubisoft y muchos más. También vendemos servicio de templates para páginas de facebook y video intros para tus videos. (del mismo dueño de Bitcoin2CDKey.com).

- cPanel-Host: cPanel hosting (Fantastico, Softaculous) y registro de dominios, certificados SSL: Destinos: Estados Unidos y Europa
- L3server: servidores dedicados y servidor virtual privado (VPS), ubicaciones: Estados Unidos y Europa
- Bitcoin Tree: Sistemas Colaborativos de Marketing Multinivel y Fondos Comunes; permiten a la Comunidad promocionar Bitcoin y ganar significativas sumas de dinero con ello.
- IberHosting.net: Alojamiento web, resellers y dominios.
- Cd Key ARG: Venta de CD KEY en Oferta, códigos de videojuegos Originales, Descarga Digital (Debe consultar la cotización en bitcoins).

Argentina

- WPLG: Diseño Gráfico. Logotipos, Publicidad, volantes. Insertados desde 2005 en el Mercado.
- Sirensis: Desarrollo Web, PHP.
- Cd Key ARG: Venta de CD KEY en Oferta, códigos de videojuegos Originales, Descarga Digital (Debe consultar la cotización en bitcoins).

Chile

- BitcoinsChile.cl: Comercio de divisas en moneda local (CLP)
- TradeHill.com: Comercio de divisas en moneda local (CLP) *Inactivo*

Costa Rica

- Tostarte: ¡publicidad creativa servida en pan tostado con mantequilla!.
- *Gnu Compu Monster*: Servicios informaticos basados en Software Libre para el hogar.

España

- Lagar la Primilla: Lagar con vinos artesanos y aceite de oliva
- SpicesCave.com: Tienda Online donde comprar especias de todo el mundo (Europa, Asia, África, América), tés, rooibos y sales (no cobran gastos de envío), página de ayuda
- BitDomain.BIZ: Registrar dominios completamente anónimo.

- NESTORGAMES: Juegos de mesa ligeros y portables (físicos, no digitales). Más de 60 diferentes.
- Morrotel: Proveedor VoIP (Llamadas SIP y acceso indirecto mediante números fijos y móviles).
- TelePienso.com: Comida para animales (perros, gatos,...). Envíos a España (incl. Canarias) y Portugal.
- YoUsoBitcoin.eu: Articulos publicitarios Bitcoin con la intención de popularizar su uso atraves de las tiendas on-line.
- Altamira21.com: Web Inmobiliaria con más de 3.000 inmuebles en Cantabria y Norte de España.
- CantabriaRustica.com: Web especializada en la venta de inmuebles rústicos y singulares en Cantabria.
- Oxcars-2011: Entradas para la cuarta edición de los Oxcars: el mayor evento de cultura libre de todos los tiempos.
- Bitcoin España: Grupo de Facebook para usuarios de Bitcoin en España.
- Mimetix: Diseño Web, Tiendas online, Posicionamiento y Marketing Online.
- Deportes Pineda (OSM): Todo para la pesca deportiva y profesional, electrónica náutica y productos para todas las modalidades de pesca.
- Sex Shop Ogges: Tienda erótica con miles de productos y Discreción garantizada.
- MaisMedia Optimización Web Marketing: Consultoría Web e Internet Marketing - Desarrollo y Optimización Web para ser encontrado en Internet.
- Nebli Centro de Halcones: Criadero de Aves Rapaces, Cursos, Material de Cetreria y Controles de Fauna.
- SOLIGAIA - Mundo Natural: Herboristeria online, dietetica, cosmetica natural y productos naturales seleccionados.
- ZAS robapinzas.com: Ropa, bisutería, complementos, calzado, piercing y decoración en un estilo hippie étnico alternativo. Venta a particulares y mayorista. Acepta Bitcoin para clientes profesionales (venta mayorista).
- ElInformatico.org: Servicios profesionales informáticos en Internet, hosting, correo, desarrollos web y posicionamiento para PYMES y particulares.
- SexShop21.com: SexShop con más de 1000 productos eróticos y envíos a toda España (inc Canarias, Ceuta y Melilla). Envíos discretos en 24/48h. **10% de Descuento en pagos con Bitcoins**
- Tximino Art: Tximino Art es una tienda online especializada en Art Toys, libros ilustrados, comics de autor y mucho más.

México

- Tabita.com.mx - Repostería, Cocina y Artesanías: Manufactura y venta de muffins, cupcakes, galletas, pasteles y otros productos de repostería, hechos de manera casera con los mejores ingredientes y con recetas exclusivas.
- Pagabitcoin.com - Pago de servicios y recargas telefónicas: Recargas telefónicas en las principales compañías mexicanas, como Telcel, Movistar, Unefon, Iusacel y Nextel.
- OpticalCube.com - Hospedaje web y servicios de TI: Hospedaje web y renta de servidores virtuales y físicos. Servicios de desarrollo de aplicaciones Web.
- Consultoría en contabilidad y finanzas: Servicios financieros y contables para personas físicas o empresas.
- Clases de francés: Clases individuales de francés en la ciudad de Oaxaca.
- Fantastico/Comicastle: Comics importados y naciones, compraventa de bitcoins.
- Webario: Cursos sobre programacion y html.
- Tiempo aire: venta de tiempo aire Telcel.
- El Diablo y la Sandía. Bonito y acogedor "Bed and Breakfast" en la ciudad de Oaxaca, México. Se ubica en el centro, a unas cuadras del zócalo (plaza principal).
- www.bitcoinplus.mx: Compra y venta de bitcoins, rifas, listado de comercios locales, saber más.

Panamá

- WM-Center: Compra, venta e intercambio de Bitcoins en Suramérica (Panamá, Ecuador), Europa y otros países. 24/7/365 soporte en español, inglés y ruso.

Venezuela

- BitWorldPoker Texas Hold'em Poker: Sitio Online para jugar al póker con Bitcoin 1btc = 10000 fichas, tenemos casino regístrate ya es gratis.

Trabajar

- Gold Line International International Financial Mutual Aid System

II. Alt-coins. Fuente: http://www.criptomonedas.org/altcoins-monedas-alternativas/

2009

Bitcoin	2009-01-03	https://bitcoinfoundation.org/

2011

Namecoin	2011-04-19	http://namecoin.info/
Ixcoin	2011-05-07	http://ixcoin.org/
Litecoin	2011-10-07	https://litecoin.org/es

2012

BBQCoin	2012-07-13	http://bbqcoin.org/
PPCoin	2012-08-16	https://ppcoin.d7.lt/
Terracoin	2012-10-26	http://terracoin.org/

2013

Novacoin	2013-02-09	http://novacoin.org/
Bytecoin	2013-04-01	http://www.bytecoin.biz/

Mincoin	2013-04-03	http://www.min-coin.org/
Feathercoin	2013-04-16	http://feathercoin.com/
Smallchange	2013-04-21	
Chinacoin	2013-04-30	
Bitbar	2013-05-01	http://www.bitbar.biz/
Junkcoin	2013-05-03	http://jkcoin.com/
YACoin	2013-05-08	http://www.yacoin.org/
Phenixcoin	2013-05-08	http://com-http.us/ccdir/pxc/
Royalcoin	2013-05-08	http://royalcoin.net/
Franko	2013-05-10	http://frankos.org/
Powercoin	2013-05-10	http://powercoin.net/
Elacoin	2013-05-14	http://elacoin.org/
Worldcoin	2013-05-14	http://www.worldcoinfoundation.org/

Goldcoin	2013-05-14	http://gldcoin.com/
Bitgem	2013-05-16	http://www.bitgem.info/
Copperlark	2013-05-16	https://copperlark.com
Nibble	2013-05-18	
Digitalcoin	2013-05-20	http://digitalcoin.co/en/
Luckycoin	2013-05-22	
Memecoin	2013-05-25	http://memecoin.org/
Americancoin	2013-05-28	http://amccoin.com/
Fastcoin	2013-05-28	http://www.fastcoin.ca/
Hypercoin	2013-05-28	
EZCoin	2013-05-29	
Megacoin	2013-06-01	http://www.megacoin.co.nz/
Noirbits	2013-06-06	http://www.noirbits.com/

Stablecoin	2013-06-07	http://stablecoin.net/
Craftcoin	2013-06-12	http://craftcoin.net/
Onecoin	2013-06-13	http://onecoin.org/
Bottlecaps	2013-06-22	http://www.bottlecaps.de/index/
Primecoin	2013-07-05	http://primecoin.org/
Cloudcoin	2013-07-24	http://cloudcoin.webs.com/